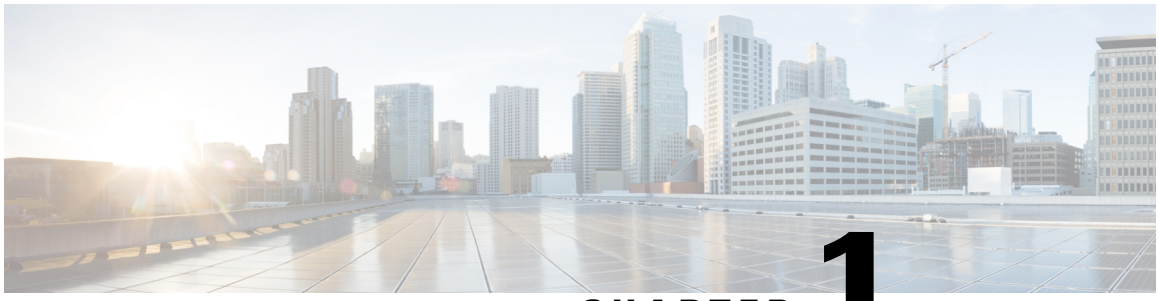
IP SLAs Configuration Guide, Cisco IOS Release 15M&T

First Published: 2012-11-21

Last Modified: 2013-03-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

IP SLAs Overview

This module describes IP Service Level Agreements (SLAs). IP SLAs allows Cisco customers to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLAs uses active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. Using IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist administrators with network troubleshooting. IP SLAs can be accessed using the Cisco software commands or Simple Network Management Protocol (SNMP) through the Cisco Round-Trip Time Monitor (RTTMON) and syslog Management Information Bases (MIBs).

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.

Information About IP SLAs

IP SLAs Technology Overview

Cisco IP SLAs uses active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. IP SLAs sends data across the network to measure performance

between multiple network locations or across multiple network paths. It simulates network data and IP services, and collects network performance information in real time. The information collected includes data about response time, one-way latency, jitter (interpacket delay variance), packet loss, voice quality scoring, network resource availability, application performance, and server response time. IP SLAs performs active monitoring by generating and analyzing traffic to measure performance either between Cisco devices or from a Cisco device to a remote IP device such as a network application server. Measurement statistics provided by the various IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Using IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance for new or existing IP services and applications. IP SLAs uses unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements.

Depending on the specific IP SLAs operation, statistics of delay, packet loss, jitter, packet sequence, connectivity, path, server response time, and download time can be monitored within the Cisco device and stored in both CLI and SNMP MIBs. The packets have configurable IP and application layer options such as a source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), a Virtual Private Network (VPN) routing/forwarding instance (VRF), and a URL web address.

Being Layer-2 transport independent, IP SLAs can be configured end-to-end over disparate networks to best reflect the metrics that an end-user is likely to experience. Performance metrics collected by IP SLAs operations include the following:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time
- Voice quality scores

Because IP SLAs is accessible using SNMP, it also can be used by performance monitoring applications like CiscoWorks Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products. For details about network management products that use IP SLAs, see http://www.cisco.com/go/ipsla .

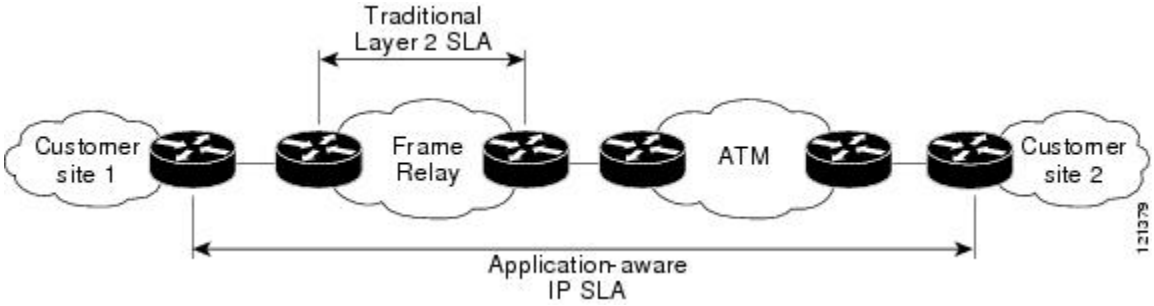
SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IP SLAs operations running on the Cisco devices. For a complete description of the object variables referenced by the IP SLAs feature, refer to the text of the CISCO-RTTMON-MIB.my file, available from the Cisco MIB website .

Service Level Agreements

Internet commerce has grown significantly in the past few years as the technology has advanced to provide faster, more reliable access to the Internet. Many companies now need online access and conduct most of their business online and any loss of service can affect the profitability of the company. Internet service providers (ISPs) and even internal IT departments now offer a defined level of service--a service level agreement--to provide their customers with a degree of predictability.

The latest performance requirements for business-critical applications, voice over IP (VoIP) networks, audio and visual conferencing, and VPNs are creating internal pressures on converged IP networks to become optimized for performance levels. Network administrators are increasingly required to support service level agreements that support application solutions. The figure below shows how IP SLAs has taken the traditional concept of Layer 2 service level agreements and applied a broader scope to support end-to-end performance measurement, including support of applications.

Figure 1: Scope of Traditional Service Level Agreement Versus IP SLAs



IP SLAs provides the following improvements over a traditional service level agreement:

- End-to-end measurements--The ability to measure performance from one end of the network to the other allows a broader reach and more accurate representation of the end-user experience.
- Sophistication--Statistics such as delay, jitter, packet sequence, Layer 3 connectivity, and path and download time that are broken down into bidirectional and round-trip numbers provide more data than just the bandwidth of a Layer 2 link.
- Ease of deployment--Leveraging the existing Cisco devices in a large network makes IP SLAs easier and cheaper to implement than the physical probes often required with traditional service level agreements.
- Application-aware monitoring--IP SLAs can simulate and measure performance statistics generated by applications running over Layer 3 through Layer 7. Traditional service level agreements can only measure Layer 2 performance.
- Pervasiveness--IP SLAs support exists in Cisco networking devices ranging from low-end to high-end devices and switches. This wide range of deployment gives IP SLAs more flexibility over traditional service level agreements.

When you know the performance expectations for different levels of traffic from the core of your network to the edge of your network, you can confidently build an end-to-end application-aware service level agreement.

Benefits of IP SLAs

- IP SLAs monitoring
  - Provides service level agreement monitoring, measurement, and verification.
- Network performance monitoring
  - Measures the jitter, latency, or packet loss in the network.
  - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment
  - Verifies that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring
  - Provides proactive verification and connectivity testing of network resources (for example, indicates the network availability of a Network File System (NFS) server used to store business critical data from a remote site).
- Troubleshooting of network operation
  - Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Voice over IP (VoIP) performance monitoring
- Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) performance monitoring and network verification

Network Performance Measurement Using IP SLAs

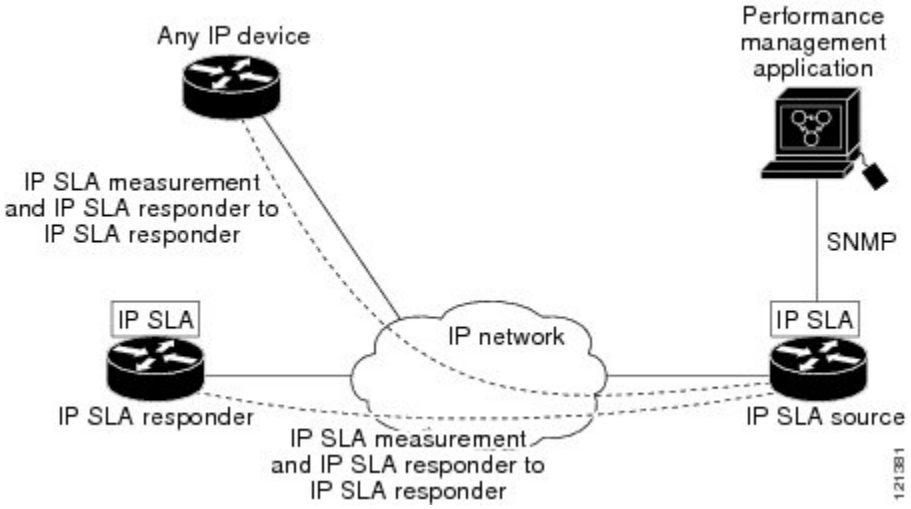
Using IP SLAs, a network engineer can monitor the performance between any area in the network: core, distribution, and edge. Monitoring can be done anytime, anywhere, without deploying a physical probe.

The IP SLAs Probe Enhancements feature is an application-aware synthetic operation agent that monitors network performance by measuring response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, for problem analysis, and for designing network topologies.

IP SLAs uses generated traffic to measure network performance between two networking devices. The figure below shows how IP SLAs starts when the IP SLAs device sends a generated packet to the destination device. After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An

IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.

Figure 2: IP SLAs Operations



To implement IP SLAs network performance measurement you need to perform these tasks:

1. Enable the IP SLAs Responder, if appropriate.
2. Configure the required IP SLAs operation type.
3. Configure any options available for the specified IP SLAs operation type.
4. Configure threshold conditions, if required.
5. Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using Cisco software commands or an NMS system with SNMP.

IP SLAs Operation Types

The various types of IP SLAs operations include the following:

- Data Link Switching Plus (DLSw+)
- Domain Name System (DNS)
- Dynamic Host Control Protocol (DHCP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- ICMP echo
- ICMP jitter
- ICMP path echo

- ICMP path jitter
- Real-Time Transport Protocol (RTP)-based VoIP
- Transmission Control Protocol (TCP) connect
- UDP echo
- UDP jitter
- UDP jitter for VoIP
- VoIP gatekeeper registration delay
- VoIP post-dial delay

IP SLAs Responder and IP SLAs Control Protocol

The IP SLAs Responder is a component embedded in the destination Cisco routing device that allows the system to anticipate and respond to IP SLAs request packets. The IP SLAs Responder provides an enormous advantage with accurate measurements without the need for dedicated probes and additional statistics not available via standard ICMP-based measurements. The patented IP SLAs Control Protocol is used by the IP SLAs Responder providing a mechanism through which the responder can be notified on which port it should listen and respond. Only a Cisco device can be a source for a destination IP SLAs Responder.

The figure "IP SLAs Operations" in the "Network Performance Measurement Using IP SLAs" section shows where the IP SLAs Responder fits in relation to the IP network. The IP SLAs Responder listens on a specific port for control protocol messages sent by an IP SLAs operation. Upon receipt of the control message, the responder will enable the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. The responder disables the port after it responds to the IP SLAs packet, or when the specified time expires. For added security, MD5 authentication for control messages is available.

Enabling the IP SLAs Responder on the destination device is not required for all IP SLAs operations. For example, if services that are already provided by the destination device (such as Telnet or HTTP) are chosen, the IP SLAs Responder need not be enabled. For non-Cisco devices, the IP SLAs Responder cannot be configured and IP SLAs can send operational packets only to services native to those devices.

Response Time Computation for IP SLAs

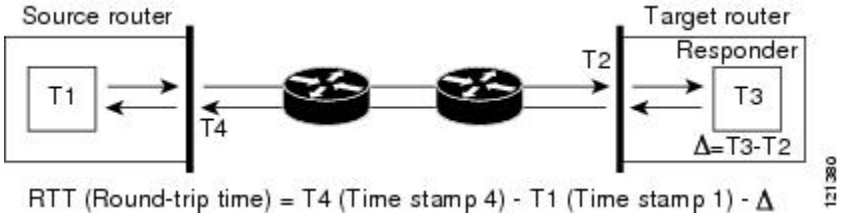
Devices may take tens of milliseconds to process incoming packets, due to other high-priority processes. This delay affects the response times because the reply to test packets might be sitting on queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if IP SLAs Responder is being used), in order to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays.

When enabled, the IP SLAs Responder allows the target device to take two time stamps both when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. At times of high network activity, an ICMP ping test often shows a long and inaccurate response time, while an IP SLAs test shows an accurate response time due to the time stamping on the responder.

The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is

subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.

Figure 3: IP SLAs Responder Time Stamping



An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements the configuration of both the source device and target device with Network Time Protocol (NTP) is required. Both the source and target need to be synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

IP SLAs Operation Scheduling

After an IP SLAs operation has been configured, you must schedule the operation to begin capturing statistics and collecting error information. When scheduling an operation, it can start immediately or start at a certain month, day, and hour. There is a pending option to set the operation to start at a later time. The pending option is also an internal state of the operation visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

Multioperations scheduling allows you to schedule multiple IP SLAs operations using a single Cisco software command or the CISCO RTTMON-MIB. This feature allows you to control the amount of IP SLAs monitoring traffic by scheduling the operations to run at evenly distributed times. This distribution of IP SLAs operations helps minimize the CPU utilization and thereby enhances the scalability of the network.

For more details about the IP SLAs multioperations scheduling functionality, see the "IP SLAs-Multioperation Scheduling of IP SLAs Operations" module of the *IP SLAs Configuration Guide* .

IP SLAs Operation Threshold Monitoring

To support successful service level agreement monitoring or to proactively measure network performance, threshold functionality becomes essential. Consistent reliable measurements immediately identify issues and can save troubleshooting time. To confidently roll out a service level agreement you need to have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as the following:

- Connection loss
- Timeout
- Round-trip time threshold

- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency

Alternately, an IP SLAs threshold violation can trigger another IP SLAs operation for further analysis. For example, the frequency could be increased or an ICMP path echo or ICMP path jitter operation could be initiated for troubleshooting.

Determining the type of threshold and the level to set can be complex, and it depends on the type of IP service being used in the network. For more details on using thresholds with IP SLAs operations, see the "IP SLAs-Proactive Threshold Monitoring of IP SLAs Operations" module of the *IP SLAs Configuration Guide* .

MPLS VPN Awareness

The IP SLAs MPLS VPN Awareness feature provides the capability to monitor IP service levels within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Using IP SLAs within MPLS VPNs allows service providers to plan, provision, and manage IP VPN services according to the service level agreement for a customer. IP SLAs operations can be configured for a specific VPN by specifying a VPN routing and forwarding (VRF) name.

History Statistics

IP SLAs maintains the following three types of history statistics:

- Aggregated statistics--By default, IP SLAs maintains two hours of aggregated statistics for each operation. Value from each operation cycle is aggregated with the previously available data within a given hour. The Enhanced History feature in IP SLAs allows for the aggregation interval to be shorter than an hour.
- Operation snapshot history--IP SLAs maintains a snapshot of data for each operation instance that matches a configurable filter, such as all, over threshold, or failures. The entire set of data is available and no aggregation takes place.
- Distribution statistics--IP SLAs maintains a frequency distribution over configurable intervals. Each time IP SLAs starts an operation, a new history bucket is created until the number of history buckets matches the specified size or the lifetime of the operation expires. By default, the history for an IP SLAs operation is not collected. If history is collected, each bucket contains one or more history entries from the operation. History buckets do not wrap.

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

Standards	Title
ITU-T G.711 u-law and G.711 a-law	Pulse code modulation (PCM) of voice frequencies
ITU-T G.729A	Reduced complexity 8 kbit/s CS-ACELP speech codec

MIBs

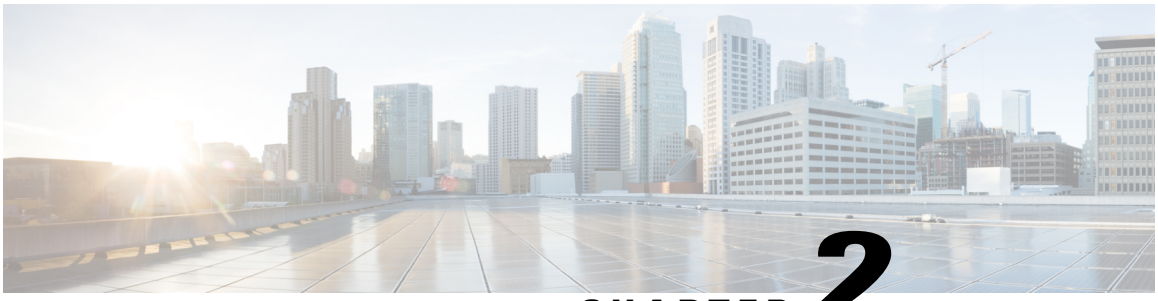
MIBs	MIBs Link
CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

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



CHAPTER 2

Configuring Auto IP SLAs in IP SLAs Engine 3.0

This document describes the auto IP Service Level Agreements (SLAs) function in IP SLAs Engine 3.0, including the following:

- Auto-measure groups--Each template, endpoint list, and scheduler can be configured once and then combined to create auto-measure groups for multiple operations, including operations for proactive threshold monitoring.
- Automatic registration--Cisco devices can be configured to automatically register with the source, which enables the source to discover the destination's address for building an endpoint list.
- Quality of service (QoS) performance--Support for active measurement of QoS.

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.

Prerequisites for Auto IP SLAs in IP SLAs Engine 3.0

- Your IP network is operational and you can access the destination device.
- If you are using a Cisco IP SLAs Responder on the destination device for any auto IP SLAs operation, the responder must be enabled before you configure the IP SLAs operation. The following operations require that an IP SLAs responder be enabled on the destination device:
  - UDP Echo
  - UPD Jitter
  - VoIP UDP

Restrictions for Auto IP SLAs in IP SLAs Engine 3.0

General Restrictions

- Auto IP SLAs is supported in IPv4 networks only.
- Only the following operation types are supported by auto IP SLAs in Cisco IP SLAs Engine 3.0:
  - Internet Control Message Protocol (ICMP) Echo
  - ICMP Jitter
  - TCP Connect
  - Internet User Datagram Protocol (UDP) Echo
  - UDP Jitter
- If you do not configure and apply a template to an auto-measure group, the default type of operation for the group is ICMP jitter.

UDP Jitter Operations Restrictions

- The 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 will be zero.
- Time synchronization is required between the source and the destination in order to provide accurate one-way delay (latency) measurements. To configure Network Time Protocol (NTP) on the source and destination, perform the tasks in the “Performing Basic System Management” chapter of the *Cisco IOS Network Management Configuration Guide* . Time synchronization is not required for one-way jitter and packet loss measurements. If the time is not synchronized between the source and destination, 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.

- 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.
- 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** command change does not increase the value beyond two hours.
- The CISCO-DATA-COLLECTION-MIB can be used to collect historical data for the operation. For information about the CISCO-DATA-COLLECTION-MIB, see http://www.cisco.com/go/mibs .

UDP Jitter Codec Operations Restrictions

- Cisco IOS IP SLAs Engine 3.0 supports only the following speech codecs:
  - G.711 a-law, 64 kbps PCM compression method
  - G.711 mu-law, 64 kbps PCM compression method
  - G.729A, 8 kbps CS-ACELP compression method
- An IP SLAs UDP jitter codec operation for analyzing VoIP SLAs will fail if control protocol is disabled.
- The **show auto template**command for UDP jitter lists the values for the "Number of statistic distribution buckets kept" and "Statistic distribution interval (milliseconds)," but these values do not apply to UDP jitter codec operations.

Proactive Threshold Measuring Restrictions

- RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).
- SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation. Only syslog messages are supported for RTTAvg threshold violations.
- Only syslog messages are supported for RTT violations during Jitter operations.
- Only SNMP traps are supported for RTT violations during non-Jitter operations.
- Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.
- Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

Auto-Measure Group Restrictions

- Only one auto IP SLAs template can be specified for each auto-measure group. Each template can be referenced by more than one group. If no template is specified for an auto-measure group, the operation type for the group is ICMP jitter by default.

- Only one auto IP SLAs endpoint list can be specified for each auto-measure group. Each endpoint list can be referenced by more than one group.
- Only one auto IP SLAs scheduler can be specified for each auto-measure group. Each scheduler can be referenced by more than one group to create a multioperations schedule.
- You cannot modify the configuration of an auto-measure group if the scheduler specified for the group is configured with a start time other than the default (pending). To avoid conflicts when you configure an auto-measure group, issue the **schedule** command last.

Information About Auto IP SLAs in IP SLAs Engine 3.0

Auto IP SLAs for Analyzing IP SLAs Operations

Auto IP SLAs in Cisco IOS IP SLAs Engine 3.0 consists of the following components:

- Endpoint list--A collection of destination endpoint addresses that can be manually configured or automatically discovered.
- Template--A set of parameters that define a single operation. You can combine any template with any endpoint list and apply the combination across many groups.
- Scheduler--Defines parameters for scheduling an operation including start time, frequency, life, age out, and probe interval. The scheduler can be associated with one or more groups.
- Auto-measure group--Created by combining one auto IP SLAs endpoint list, template, and scheduler. You can combine any template with any endpoint list and any scheduler and apply the combination across many groups.

When the group is scheduled to run, based on the scheduler, one IP SLAs operation is created for each destination address in the endpoint list. The operation type depends on the template in the group. If the group is deleted or unscheduled, the created IP SLAs operations are removed.

For configuration information, see the "How to Configure Auto IP SLAs in Cisco IOS IP SLAs Engine 3.0" section.

QoS Integration for Auto IP SLAs

QoS integration allows for active measurement of QoS performance and enables customers to test network readiness for the deployment of high priority, low latency traffic that is generated by applications such as voice and video. Auto IP SLAs traffic is marked with the appropriate Differentiated Services Code Point (DSCP) marker and then sends out the required interface.

Automatic Registration of Destinations for Auto IP SLAs Operations

Destination Cisco devices and Cisco IOS IP SLAs Responders in Cisco devices can be configured to automatically register with the source. The source will discover the destination's address and put it in an endpoint list.

How to Configure Auto IP SLAs in IP SLAs Engine 3.0

Configuring Automatic Registration of Responder on the Destination Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder auto-register** {*source-ipaddress*|*source-hostname*} [**client-id** *client-id*] [**endpoint-list** *template-name*] [**retry-timer** *minutes*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla responder auto-register** {*source-ipaddress*|*source-hostname*} [**client-id** *client-id*] [**endpoint-list** *template-name*] [**retry-timer** *minutes*] **Example:** `Router(config)# ip sla responder auto-register 10.1.1.23 endpoint-list autolist`	Enables destination to register with source.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an Endpoint List on the Source Device

Perform one of the following tasks:

Using Automatic Registration to Configure an Endpoint List

Before You Begin

XThe destination device or responder must be configured for auto registration. For configuration information, see the "Configuring Automatic Registration of Responder on the Destination Device" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto discovery**
4. **ip sla auto endpoint-list type ip** *template-name*
5. **description** *description*
6. **discover** [**port** *port*]
7. **access-list** {*standard-range* | *expanded-range*}
8. **ageout** *seconds*
9. **measurement-retry** *number-of-retries*
10. **end**
11. show ip sla auto discovery

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto discovery** **Example:** `Router(config)# ip sla auto discovery`	Enables the source to discover the responder endpoints.

	Command or Action	Purpose
Step 4	**ip sla auto endpoint-list type ip** *template-name* **Example:** `Router(config)# ip sla auto endpoint-list type ip autolist`	Begins configuring an endpoint list and enters endpoint-list configuration mode.
Step 5	**description** *description* **Example:** `Router(config-epl)# description testing discovery`	(Optional) Adds descriptive text to the template being configured.
Step 6	**discover** [**port** *port*] **Example:** `Router(config-epl)# discover`	Automatically discovers the IP addresses and port numbers of endpoints on the destination and enters endpoint-list auto-discovery configuration mode.
Step 7	**access-list** {*standard-range* | *expanded-range*} **Example:** `Router(config-epl-disc)# access-list 1`	Names and adds the list of discovered IP addresses to the endpoint list being configured.
Step 8	**ageout** *seconds* **Example:** `Router(config-epl-disc)# ageout 10`	(Optional) Sets an ageout timer.
Step 9	**measurement-retry** *number-of-retries* **Example:** `Router(config-epl-disc)# measurement-retry 10`	(Optional) Specifies the number of times to retry after an operation fails.
Step 10	**end** **Example:** `Router(config-ep-disc)# end`	Returns to privileged EXEC mode.
Step 11	show ip sla auto discovery **Example:** `Router# show ip sla auto discovery`	(Optional) Displays status of auto-discovery.

Manually Configuring an Endpoint List

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto endpoint-list type ip** *template-name*
4. **description** *description*
5. **ip-address** *address* [**-** *address* | **,** *...* **,** *address*] **port** *port*
6. **end**
7. **show ip sla auto** [**type ip** [*template-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto endpoint-list type ip** *template-name* **Example:** `Router(config)# ip sla auto endpoint-list type ip edgehosts-epl`	Begins configuring an endpoint list and enters endpoint-list configuration mode.
Step 4	**description** *description* **Example:** `Router(config-epl)# description manual config`	(Optional) Adds descriptive text to the template being configured.
Step 5	**ip-address** *address* [**-** *address*	**,** *...* **,** *address*] **port** *port* **Example:** `Router(config-epl)# ip-address 10.1.1.1-13 port 6500`	Adds the IP addresses of endpoints to the endpoint list being configured. • Use the **no** from of this command to modify the endpoint list by removing one or more addresses. • Repeat this command until all desired addresses are configured.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-epl)# end`	Returns to privileged EXEC mode.
Step 7	**show ip sla auto** [**type ip** [*template-name*]] **Example:** `Router# show ip sla auto type ip edgehosts-epl`	(Optional) Displays the configuration of the endpoint list.

Configuring a Scheduler on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto schedule** *schedule-id*
4. **ageout** *seconds*
5. **frequency** {*seconds* | **range** *random-frequency-range*}
6. **life** {**forever** | *seconds*}
7. **probe-interval** *milliseconds*
8. **start-time** {*hh* **:** *mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}
9. **end**
10. **show ip sla auto schedule** [*schedule-id*]

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip sla auto schedule** *schedule-id* **Example:** `Router(config)# ip sla auto schedule theschedule`	Begins configuring a scheduler and enters IP SLA auto-measure schedule configuration mode.
Step 4	**ageout** *seconds* **Example:** `Router(config-am-schedule)# ageout 43200`	(Optional) Sets an ageout timer for inactive operations.
Step 5	**frequency** {*seconds* | **range** *random-frequency-range*} **Example:** `Router(config-am-schedule)# frequency 60`	(Optional) Specifies either the frequency timer or random frequency range for multiple operations.
Step 6	**life** {**forever** | *seconds*} **Example:** `Router(config-am-schedule)# life 43200`	(Optional) Defines the lifetime of the operation.
Step 7	**probe-interval** *milliseconds* **Example:** `Router(config-am-schedule)# probe-interval 200`	(Optional) Specifies the interval for multiple operations.
Step 8	**start-time** {*hh* **:** *mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*} **Example:** `Router(config-am-schedule)# start-time now`	(Optional) Specifies the start time of an operation.
Step 9	**end** **Example:** `Router(config-am-schedule)# end`	Returns to privileged EXEC mode.
Step 10	**show ip sla auto schedule** [*schedule-id*] **Example:** `Router# show ip sla auto schedule`	(Optional) Displays the configuration of the scheduler.

Configuring a Template on the Source Device

Note If you do not configure and apply a template to an auto-measure group, the default type of operation for the group is ICMP jitter.

Configuring an ICMP Echo Operation

Perform one of the following tasks:

Configuring a Template for a Basic ICMP Echo Operation

Note We recommend using a Cisco networking device as the destination device although any networking device that supports RFC 862, *Echo protocol* , can be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip icmp-echo** *template-name*
4. **description** *description*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip sla auto template type ip icmp-echo** *template-name* **Example:** `Router(config)# ip sla auto template type ip icmp-echo tmp-icmpecho`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-icmp-ech)# description default oper temp for icmp echo`	(Optional) Adds descriptive text to the template being configured.
Step 5	**end** **Example:** `Router(config-tplt-icmp-ech)# end`	Returns to global configuration mode.

Example

The following output shows the configuration, including default values, of a template for an ICMP echo operation:

```
Router# show
 ip sla auto template type ip icmp-echo
IP SLAs Auto Template: tpl-icmplecho
    Measure Type: icmp-echo (control enabled)
    Description: default oper temp for icmp echo
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 16   Verify Data: false
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the “Adding Proactive Threshold Monitoring to a Template on the Source Device” section. Otherwise, see the “Configuring an Auto-Measure Group on the Source Device” section.

Configuring an ICMP Echo Operation Template with Additional Characteristics

Note We recommend using a Cisco networking device as the destination device although any networking device that supports RFC 862, *Echo Protocol* , can be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip icmp-echo** template-name
4. **description** *description*
5. **source-ip** {*ip-address* | *hostname*}
6. **tos** *number*
7. **vrf** *vrf-name*
8. **parameters**
9. **history buckets-kept** *size*
10. **history distributions-of-statistics-kept** *size*
11. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
12. **history filter** {**none** | **all** | **overThreshold** | **failures**}
13. **history hours-of-statistics-kept** *hours*
14. **history lives-kept** *lives*
15. **history statistics-distribution-interval** *milliseconds*
16. **request-data-size** *bytes*
17. **threshold** *milliseconds*
18. **timeout** *milliseconds*
19. **verify-data**
20. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip sla auto template type ip icmp-echo** template-name **Example:** `Router(config)# ip sla auto template type ip icmp-echo icmp_echo_2`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-icmp-ech)# description custom icmp echo template`	(Optional) Adds descriptive text to the template being configured.
Step 5	**source-ip** {*ip-address* | *hostname*} **Example:** `Router(config-tplt-icmp-ech)# source-ip 172.29.139.132`	(Optional) Specifies the source for the operation.
Step 6	**tos** *number* **Example:** `Router(config-tplt-icmp-ech)# tos 160`	(Optional) Defines the Type of Service (ToS) byte in the IPv4 header of an IP SLAs operation.
Step 7	**vrf** *vrf-name* **Example:** `Router(config-tplt-icmp-ech)# vrf vpn-A`	(Optional) Allows monitoring within MultiProtocol Label Switching (MPLS) VPNs using IP SLAs operations.
Step 8	**parameters** **Example:** `Router(config-tplt-icmp-ech)# parameters`	(Optional) Enters IP SLA template parameters configuration mode.
Step 9	**history buckets-kept** *size* **Example:** `Router(config-icmp-ech-params)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 10	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-icmp-ech-params)# 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 11	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Router(config-icmp-ech-params)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 12	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-icmp-ech-params)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 13	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-icmp-ech-params)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 14	**history lives-kept** *lives* **Example:** `Router(config-icmp-ech-params)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 15	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-icmp-ech-params)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	**request-data-size** *bytes* **Example:** `Router(config-icmp-ech-params)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 17	**threshold** *milliseconds* **Example:** `Router(config-icmp-ech-params)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	**timeout** *milliseconds* **Example:** `Router(config-icmp-ech-params)# 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 19	**verify-data** **Example:** `Router(config-icmp-ech-params)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption. **Note** Use this command with caution during normal operations.
Step 20	**end** **Example:** `Router(config-icmp-ech-params)# end`	Returns to privileged EXEC mode.

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring an ICMP Jitter Operation

Perform one of the following tasks:

Configuring a Template for a Basic ICMP Jitter Operation

Note

- When compared to the IP SLAs 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 Operation Sore (MOS), Calculated Planning Impairment Factor (ICPIF), or estimated transmission rating factor (R-factor) reaction configuration capabilities.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip icmp-jitter** *template-name*
4. **description** *description*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip icmp-jitter** *template-name* **Example:** `Router(config)# ip sla auto template type ip icmp-jitter basic_icmp_jitter`	Begins configuring the template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-icmp-jtr)# description default oper temp for icmp-jitter`	(Optional) Adds descriptive text to the template being configured.
Step 5	**end** **Example:** `Router(config-tplt-icmp-jtr)# end`	Returns to privileged EXEC mode.

Example

The following output shows the configuration, including default values, of a template for a basic ICMP jitter operation:

```
Router# show ip sla auto template type ip icmp-jitter
IP SLAs Auto Template: basic_icmp_jitter
    Measure Type: icmp-jitter
    Description: default oper temp for icmp jitter
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
```

```
    Max number of distributions buckets: 1
Reaction Configuration: None
```

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring an ICMP Jitter Operation Template with Additional Characteristics

Note

- When compared to the IP SLAs 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 MOS, ICPIF, or estimated R-factor reaction configuration capabilities.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip icmp-jitter** *template-name*
4. **description** *description*
5. **source-ip** {*ip-address* | *hostname*}
6. **tos** *number*
7. **vrf** *vrf-name*
8. **parameters**
9. **history distributions-of-statistics-kept** *size*
10. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
11. **history filter** {**none** | **all** | **overThreshold** | **failures**}
12. **history hours-of-statistics-kept** *hours*
13. **history statistics-distribution-interval** *milliseconds*
14. **interval** *milliseconds*
15. **num-packet** *packet-number*
16. **threshold** *milliseconds*
17. **timeout** *milliseconds*
18. **verify-data**
19. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip icmp-jitter** *template-name* **Example:** `Router(config)# ip sla auto template type ip icmp-jitter custom_imcp_jitter`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-icmp-jtr)# description custom icmp jitter template`	(Optional) Adds descriptive text to the template being configured.
Step 5	**source-ip** {*ip-address* | *hostname*} **Example:** `Router(config-tplt-icmp-jtr)# source-ip 10.1.2.34`	(Optional) Specifies the source for the operation.
Step 6	**tos** *number* **Example:** `Router(config-tplt-icmp-jtr)# tos 160`	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 7	**vrf** *vrf-name* **Example:** `Router(config-tplt-icmp-jtr)# vrf vpn-A`	(Optional) Allows monitoring within MPLS VPNs using IP SLAs operations.
Step 8	**parameters** **Example:** `Router(config-tplt-icmp-jtr)# parameters`	(Optional) Enters IP SLA template parameters configuration mode.

	Command or Action	Purpose
Step 9	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-icmp-jtr-params)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 10	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Router(config-icmp-jtr-params)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 11	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-icmp-jtr-params)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 12	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-icmp-jtr-params)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 13	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-icmp-jtr-params)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	**interval** *milliseconds* **Example:** `Router(config-icmp-jtr-params)# interval 40`	(Optional) Sets number of milliseconds between sent packets.
Step 15	**num-packet** *packet-number* **Example:** `Router(config-icmp-jtr-params)# num-packets 100`	(Optional) Sets number of packets to be sent.
Step 16	**threshold** *milliseconds* **Example:** `Router(config-icmp-jtr-params)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 17	**timeout** *milliseconds* **Example:** `Router(config-icmp-jtr-params)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 18	**verify-data** **Example:** `Router(config-icmp-jtr-params)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption. **Note** Use this command with caution during normal operations because it generates unnecessary overhead.
Step 19	**end** **Example:** `Router(config-icmp-jtr-params)# end`	Returns to global configuration mode.

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a TCP Connect Operation

Perform one of the following tasks:

Configuring a Template for a Basic TCP Connect Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip tcp-connect** *template-name*
4. **description** *description*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip tcp-connect** *template-name* **Example:** `Router(config)# ip sla auto template type ip tcp-connect basic_tcp_connect`	Begins configuring a template and enters IP SLA IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-tcp-conn)# description default oper temp for tcp-connect`	(Optional) Adds descriptive text to the template being configured.
Step 5	**end** **Example:** `Router(config-tplt-tcp-conn)# end`	Returns to privileged EXEC mode.

Example
The following output shows the configuration, including default values, of a template for a basic TCP connect operation:

```
Router# show ip sla auto template type ip tcp-connect
IP SLAs Auto Template: basic_tcp_connect
    Measure Type: tcp-connect (control enabled)
    Description: default oper temp for tcp-connect
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a TCP Connect Operation Template with Additional Characteristics

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip tcp-connect** *template-name*
4. **control** {**enable** | **disable**}
5. **description** *description*
6. **source-ip** {*ip-address* | *hostname*}
7. **source-port** *port-number*
8. **tos** *number*
9. **vrf** *vrf-name*
10. **parameters**
11. **history buckets-kept** *size*
12. **history distributions-of-statistics-kept** *size*
13. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
14. **history filter** {**none** | **all** | **overThreshold** | **failures**}
15. **history hours-of-statistics-kept** *hours*
16. **history lives-kept** *lives*
17. **history statistics-distribution-interval** *milliseconds*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip sla auto template type ip tcp-connect** *template-name* **Example:** `Router(config)# ip sla auto template type ip tcp-connect custom_tcp_connect`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**control** {**enable** | **disable**} **Example:** `Router(config-tplt-tcp-conn)# control enable`	(Optional) Specifies whether control messages are sent to responder before beginning the IP SLAs operation. • Default--Control is enabled.
Step 5	**description** *description* **Example:** `Router(config-tplt-tcp-conn)# description custom tcp-connect template`	(Optional) Adds descriptive text to the template being configured.
Step 6	**source-ip** {*ip-address* | *hostname*} **Example:** `Router(config-tplt-tcp-conn)# source-ip 10.1.2.34`	(Optional) Specifies the source for the operation.
Step 7	**source-port** *port-number* **Example:** `Router(config-tplt-tcp-conn)# source-port 23`	(Optional) Specifies the source port for the operation.
Step 8	**tos** *number* **Example:** `Router(config-tplt-tcp-conn)# tos 160`	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 9	**vrf** *vrf-name* **Example:** `Router(config-tplt-tcp-conn)# vrf vpn-A`	(Optional) Allows monitoring within MPLS VPNs using IP SLAs operations.
Step 10	**parameters** **Example:** `Router(config-tplt-tcp-conn)# parameters`	Enters IP SLA template parameters configuration mode.

	Command or Action	Purpose
Step 11	**history buckets-kept** *size* **Example:** `Router(config-tcp-conn-params)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 12	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-tcp-conn-params)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 13	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Router(config-tcp-conn-params)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 14	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-tcp-conn-params)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 15	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-tcp-conn-params)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 16	**history lives-kept** *lives* **Example:** `Router(config-tcp-conn-params)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 17	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-tcp-conn-params)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.

	Command or Action	Purpose
Step 18	**threshold** *milliseconds* **Example:** `Router(config-tcp-conn-params)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 19	**timeout** *milliseconds* **Example:** `Router(config-tcp-conn-params)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 20	**end** **Example:** `Router(config-tcp-conn-params)# end`	Returns to privileged EXEC mode.

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a UDP Echo Operation

Perform one of the following tasks:

Configuring a Template for a Basic UDP Echo Operation

Note We recommend using a Cisco networking device as the destination device although any networking device that supports RFC 862, *Echo Protocol* , can be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip udp-echo** *template-name*
4. **description** *description*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip udp-echo** *template-name* **Example:** `Router(config)# ip sla auto template type ip udp-echo basic_udp_echo`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-udp-ech)# description default oper temp for udp echo`	(Optional) Adds descriptive text to the template being configured.
Step 5	**end** **Example:** `Router(config-tplt-udp-ech)# end`	Returns to privileged EXEC mode.

Example

The following output shows the configuration, including default values, of a template for a basic UDP echo operation:

```
Router# show ip sla auto template type ip udp-echo
IP SLAs Auto Template: basic_udp_echo
    Measure Type: udp-echo (control enabled)
    Description: default oper temp for udp echo
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 16   Verify Data: false
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
```

```
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a UDP Echo Operation Template with Additional Characteristics

Note We recommend using a Cisco networking device as the destination device although any networking device that supports RFC 862, *Echo Protocol* , can be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip udp-echo** *template-name*
4. **description** *description*
5. **source-ip** {*ip-address* | *hostname*}
6. **source-port** port-number
7. **tos** *number*
8. **vrf** *vrf-name*
9. **parameters**
10. **history buckets-kept** *size*
11. **history distributions-of-statistics-kept** *size*
12. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
13. **history filter** {**none** | **all** | **overThreshold** | **failures**}
14. **history hours-of-statistics-kept** *hours*
15. **history lives-kept** *lives*
16. **history statistics-distribution-interval** *milliseconds*
17. **request-data-size** *bytes*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **verify-data**
21. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip udp-echo** *template-name* **Example:** `Router(config)# ip sla auto template type ip udp-echo custom_udp_echo`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-udp-ech)# description custom udp echo template`	(Optional) Adds descriptive text to the template being configured.
Step 5	**source-ip** {*ip-address* | *hostname*} **Example:** `Router(config-tplt-udp-ech)# source-ip 10.1.2.34`	(Optional) Specifies the source for the operation.
Step 6	**source-port** port-number **Example:** `Router(config-tplt-udp-ech)# source-port 23`	(Optional) Specifies the source port for the operation.
Step 7	**tos** *number* **Example:** `Router(config-tplt-udp-ech)# tos 160`	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 8	**vrf** *vrf-name* **Example:** `Router(config-tplt-udp-ech)# vrf vpn-A`	(Optional) Allows monitoring within MPLS VPNs using IP SLAs operations.

	Command or Action	Purpose
Step 9	**parameters** **Example:** `Router(config-tplt-udp-ech)# parameters`	Enters IP SLA template parameters configuration mode.
Step 10	**history buckets-kept** *size* **Example:** `Router(config-udp-ech-params)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 11	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-udp-ech-params)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 12	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Router(config-udp-ech-params)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 13	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-udp-ech-params)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 14	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-udp-ech-params)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 15	**history lives-kept** *lives* **Example:** `Router(config-udp-ech-params)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.

	Command or Action	Purpose
Step 16	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-udp-ech-params)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 17	**request-data-size** *bytes* **Example:** `Router(config-udp-ech-params)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 18	**threshold** *milliseconds* **Example:** `Router(config-udp-ech-params)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 19	**timeout** *milliseconds* **Example:** `Router(config-udp-ech-params)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 20	**verify-data** **Example:** `Router(config-udp-ech-params)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption. **Note** Use this command with caution during normal operations.
Step 21	**end** **Example:** `Router(config-udp-ech-params)# end`	Returns to privileged EXEC mode.

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a UDP Jitter Operation on the Source Device

Perform one of the following tasks:

Configuring a Template for a Basic UDP Jitter Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip udp-jitter** *template-name*
4. **description** *description*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip udp-jitter** *template-name* **Example:** `Router(config)# ip sla auto template type ip basic_udp_jitter`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-udp-jtr)# description default oper temp for udp jitter`	(Optional) Adds descriptive text to the template being configured.
Step 5	**end** **Example:** `Router(config-tplt-udp-jtr)# end`	Returns to privileged EXEC mode.

Example

The following output shows the configuration, including default values, of a template for a basic UDP jitter operation:

```
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: basic_udp_jitter
    Measure Type: udp-jitter (control enabled)
    Description: default oper temp for udp jitter
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a Template for a Basic VoIP SLAs UDP Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip udp-jitter** *template-name*
4. **codec** *codec-type* [**advantage-factor** *value*][**codec-numpackets** *number-of-packets*][**codec-interval** *milliseconds*][**codec-size** *number-of-bytes*]
5. **description** *description*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip udp-jitter** *template-name* **Example:** `Router(config)# ip sla auto template type ip voip_g711alaw`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**codec** *codec-type* [**advantage-factor** *value*][**codec-numpackets** *number-of-packets*][**codec-interval** *milliseconds*][**codec-size** *number-of-bytes*] **Example:** `Router(config-tplt-udp-jtr)# codec g711alaw`	Sets the codec for the operation being configured.
Step 5	**description** *description* **Example:** `Router(config-tplt-udp-jtr)# description oper template for voip udp`	(Optional) Adds descriptive text to the template being configured.
Step 6	**end** **Example:** `Router(config-tplt-udp-jtr)# end`	Returns to privileged EXEC mode.

Example

The following output shows the configuration, including default values, of a template for a basic VoIP SLAs UDP jitter operation:

```
Router# show ip sla auto template type ip udp-jitter voip_g711alaw
IP SLAs Auto Template: voip_g711alaw
    Measure Type: udp-jitter (control enabled)
    Description: oper template for voip udp
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Verify Data: false
        Timeout: 5000           Threshold: 5000
        Codec: g711alaw Number of packets: 1000
        Interval: 20    Payload size: 16        Advantage factor: 0
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
```

```
    Hours of statistics kept: 2
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Configuring a UDP Jitter Operation Template with or without Codec with Additional Characteristics

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip udp-jitter** *template-name*
4. **codec** *codec-type* [**advantage-factor** *value*] [**codec-numpackets** *number-of-packets*] [**codec-interval** *milliseconds*] [**codec-size** *number-of-bytes*]
5. **control** {**enable** | **disable**}
6. **description** *description*
7. **source-ip** {*ip-address* | *hostname*}
8. **source-port** *port-number*
9. **tos** *number*
10. **vrf** *vrf-name*
11. **parameters**
12. **precision** {**milliseconds** | **microseconds**}
13. **clock-tolerance ntp oneway** {**absolute** *value* | **percent** *value*}
14. **history distributions-of-statistics-kept** *size*
15. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
16. **history hours-of-statistics-kept** *hours*
17. **history statistics-distribution-interval** *milliseconds*
18. **interval** *milliseconds*
19. **num-packets** *packet-number*
20. **operation-packet-priority** {**normal** | **high**}
21. **request-data-size** *bytes*
22. **threshold** *milliseconds*
23. **timeout** *milliseconds*
24. **verify-data**
25. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip udp-jitter** *template-name* **Example:** `Router(config)# ip sla auto template type ip udp-jitter custom_udp_jitter`	Begins configuring a template and enters IP SLA template configuration mode.
Step 4	**codec** *codec-type* [**advantage-factor** *value*] [**codec-numpackets** *number-of-packets*] [**codec-interval** *milliseconds*] [**codec-size** *number-of-bytes*] **Example:** `Router(config-tplt-udp-jtr)# codec g711ulaw advantage-factor 2`	(Optional) Required for analyzing VoIP SLAs. Sets the codec for the operation being configured. **Note** You should not specify values for the interval, size, and number of packet options unless you have a specific reason to override the defaults.
Step 5	**control** {**enable** | **disable**} **Example:** `Router(config-tplt-udp-jtr)# control enable`	(Optional) Specifies whether control messages are sent to responder before beginning the IP SLAs operation. • For UDP jitter codec operations--Do not disable control protocol. • Default--Control is enabled.
Step 6	**description** *description* **Example:** `Router(config-tplt-udp-jtr)# description custom udp jitter template`	(Optional) Adds descriptive text to the template being configured.
Step 7	**source-ip** {*ip-address* | *hostname*} **Example:** `Router(config-tplt-udp-jtr)# source-ip 10.1.2.34`	(Optional) Specifies the source for the operation.

	Command or Action	Purpose
Step 8	**source-port** *port-number* **Example:** `Router(config-tplt-udp-jtr)# source-port 23`	(Optional) Specifies the source port for the operation.
Step 9	**tos** *number* **Example:** `Router(config-tplt-udp-jtr)# tos 160`	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 10	**vrf** *vrf-name* **Example:** `Router(config-tplt-udp-jtr)# vrf vpn-A`	(Optional) Allows monitoring within MPLS VPNs using IP SLAs operations.
Step 11	**parameters** **Example:** `Router(config-tplt-udp-jtr)# parameters`	(Optional) Enters IP SLA template parameters configuration mode.
Step 12	**precision** {**milliseconds** | **microseconds**} **Example:** `Router(config-udp-jtr-params)# precision microseconds`	(Optional) Sets the level of precision at which the statistics for an IP SLAs operation are measured • This command must be configured before the **clock-tolerance ntp oneway**command.
Step 13	**clock-tolerance ntp oneway** {**absolute** *value* | **percent** *value*} **Example:** `Router(config-udp-jtr-params)# clock-tolerance ntp oneway percent 100`	(Optional) Sets the acceptable NTP clock synchronization tolerance for a one-way IP SLAs operation measurement.
Step 14	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-udp-jtr-params)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 15	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Router(config-udp-jtr-params)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.

	Command or Action	Purpose
Step 16	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-udp-jtr-params)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 17	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-udp-jtr-params)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 18	**interval** *milliseconds* **Example:** `Router(config-udp-jtr-params)# interval 40`	(Optional) Specifies the interval between packets for an IP SLA jitter operation.
Step 19	**num-packets** *packet-number* **Example:** `Router(config-udp-jtr-params)# num-packets 100`	(Optional) Specifies the number of packets for an IP SLAs jitter operation.
Step 20	**operation-packet-priority** {**normal** | **high**} **Example:** `Router(config-udp-jtr-params)# operation-packet-priority high`	(Optional) Specifies the packet priority for an IP SLAs jitter operation.
Step 21	**request-data-size** *bytes* **Example:** `Router(config-udp-jtr-params)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 22	**threshold** *milliseconds* **Example:** `Router(config-udp-jtr-params)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 23	**timeout** *milliseconds* **Example:** `Router(config-udp-jtr-params)# 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 24	**verify-data** **Example:** `Router(config-udp-jtr-params)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption. **Note** Use this command with caution during normal operations.
Step 25	**end** **Example:** `Router(config-udp-jtr-params)# end`	Returns to privileged EXEC mode.

What to Do Next

To configure this auto IP SLAs template for proactive threshold monitoring, see the "Adding Proactive Threshold Monitoring to a Template on the Source Device" section. Otherwise, see the "Configuring an Auto-Measure Group on the Source Device" section.

Adding Proactive Threshold Monitoring to a Template on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto template type ip** *operation template-name*
4. **description** *description*
5. **react** [*monitored-element*[[**action-type**{*type-of-action*}] [**threshold-type**{**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy**[*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]
6. **exit**
7. **ip sla logging traps**
8. Do one of the following:
   - **snmp-server enable traps rtr**
   - **snmp-server enable traps syslog**
9. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto template type ip** *operation template-name* **Example:** `Router(config)# ip sla auto template type ip icmp-echo icmp_echo_2`	Begins configuring a template and enters the appropriate submode, based on the *operation* argument, of IP SLA template configuration mode.
Step 4	**description** *description* **Example:** `Router(config-tplt-icmp-ech)# description custom icmp echo template`	(Optional) Adds descriptive text to the template being configured.
Step 5	**react** [*monitored-element*[[**action-type**{*type-of-action*}] [**threshold-type**{**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy**[*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]] **Example:** `Router(config-tplt-icmp-ech)# react rtt action-type trapOnly threshold-type consecutive 3`	(Optional) Defines proactive threshold monitoring and reaction parameters.
Step 6	**exit** **Example:** `Router(config-tplt-icmp-ech)# exit`	Exits this configuration mode.
Step 7	**ip sla logging traps** **Example:** `Router(config)# ip sla logging traps`	(Optional) Enables IP SLAs syslog notifications from CISCO-RTTMON-MIB. • Required if the **react** command is configured with the **trapOnly** keyword.
Step 8	Do one of the following: • **snmp-server enable traps rtr**	(Optional) Enables system to generate CISCO-RTTMON-MIB traps.

	Command or Action	Purpose

	• **snmp-server enable traps syslog**
	
	Example:
	`Router(config)# snmp-server enable traps rtr`
	
	Example:
	`Router(config)# snmp-server enable traps syslog`
		or
		(Optional) Enables system to generate CISCO-SYSLOG-MIB traps.

Step 9	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 10.1.1.1 public syslog`	(Optional) Sends traps to a remote host. • Required if the**snmp-server enable traps** command is configured.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits this configuration mode and goes to privileged EXEC mode.

Configuring an Auto-Measure Group on the Source Device

Before You Begin

Before configuring an auto-measure group, you must configure the auto IP SLAs template, endpoint list, and scheduler to be specified for the auto-measure group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla auto group type ip** *group-name*
4. **description** *description*
5. **template** {**icmp-echo** | **icmp-jitter** | **tcp-connect** | **udp-echo** | **udp-jitter**} *template-name*
6. **destination** *template-name*
7. **schedule** *schedule-id*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla auto group type ip** *group-name* **Example:** `Router(config)# ip sla auto group type ip customergroup`	Begins configuring an auto-measure group and enters IP SLA auto-measure group configuration mode.
Step 4	**description** *description* **Example:** `Router(config-am-group)# description customergroup`	(Optional) Adds descriptive text to the auto-measure group being configured.
Step 5	**template** {**icmp-echo** | **icmp-jitter** | **tcp-connect** | **udp-echo** | **udp-jitter**} *template-name* **Example:** `Router(config-am-group)# template icmp-echo tmp-icmpecho`	(Optional) Specifies a template for the group being configured. • The default operation type for group is ICMP jitter.
Step 6	**destination** *template-name* **Example:** `Router(config-am-group)# destination edgehosts-epl`	Specifies an endpoint list for the group being configured.
Step 7	**schedule** *schedule-id* **Example:** `Router(config-am-group)# schedule theschedule`	Specifies a scheduler for the group being configured.
Step 8	**end** **Example:** `Router(config-am-group)# end`	Returns to privileged EXEC mode.

Configuration Examples for Auto IP SLAs in IP SLAs Engine 3.0

Example IP SLAs Auto-Measure Group

The following sample output shows the configuration of an auto-measure group (customergroup) for an ICMP echo operation as well as information about each operation that was created for each destination in the endpoint list (edgehosts-epl):

```
Router# show running-config
.
.
.
ip sla auto template type ip icmp-echo tmp-icmpecho
ip sla auto endpoint-list type ip edgehosts-epl
ip-address 10.1.1.1 port 6500
ip sla auto group type ip customergroup
schedule theschedule
template icmp-echo tmp-icmpecho
destination edgehosts-epl
ip sla auto schedule theschedule
start-time now
!
Router# show ip sla auto group

Group Name: customergroup
    Description:
    Activation Trigger: Immediate
    Destination: edgehosts-epl
    Schedule: theschedule
    Measure Template: tmp-icmpecho(icmp-echo)
IP SLAs auto-generated operations of group customergroup
  sno     oper-id         type             dest-ip-addr/port
    1   299389922      icmp-echo             10.1.1.1/NA
```

Example Configuring Auto IP SLAs Using SNMP

Example MIB Strings for Auto IP SLAs Template

This example shows the MIB string for configuring a template (tmp-icmpecho) for an ICMP echo operation.

The Cisco IOS command for creating this template is **ip sla auto template type ip** *operation template-name*.

The syntax for the MIB string to create an template is as follows:

MIBobject **.** *length-of-name* **.** *ASCII-value-for-each-character-in-name*

The period (.) between each variable is required and a period (.) is also required between each character in the *ASCII-value-for-each-character-in-the-name* argument.

The following MIB strings are for configuring the template (tmp-icmpecho) in this example. See the table below for the appropriate values for each variable in the string.

- To create the template, the MIB string is:

```
cipslaIcmpEchoTmplRowStatus.
12.
116.109.108.45.105.99.109.112.101.99.104.111 -i 4
```

- To display this configuration in the running configuration, the MIB string is:

```
cipslaIcmpEchoTmplStorageType.
12.
116.109.108.45.105.99.109.112.101.99.104.111 -i 3
```

- To configure a value of 255 for ToS in this same template, the MIB string is:

```
cipslaIcmpEchoTmplTOS.
12.
116.109.108.45.105.99.109.112.101.99.104.111 -g 255
```

Table 1: Values for MIB Strings to Create, Display, and Modify Configuration of Template

Variable	Value	Comments
MIBobject	cipslaIcmpEchoTmplRowStatus	Creates a template.
	cipslaIcmpEchoTmplStorageType	Displays MIB string in running configuration.
	cipslaIcmpEchoTmplTOS	Adds value for ToS to template.
length-of-nam e	12	To determine this value, count the number of characters in the name. The name of this template in this example is: tmp-icmpecho.
ASCII-value-for-each-character-in-name	116.109.108.45.105.99.109.112.101.99.104.111	To determine this value, replace each letter of the template name with its ASCII equivalent. Each of the ASCII characters must be separated by a period (.). The name of this template in this example is: tmp-icmpecho.

Example MIB Strings for Auto IP SLAs Endpoint List

The following example shows the MIB string for configuring an endpoint list (edgehosts-epl).

The Cisco IOS commands for configuring an endpoint list are:

- **ip sla auto endpoint-list type ip** *template-name*
- **ip-address** *ip-address* **port** *port*

The syntax for the MIB string to configure an endpoint list is as follows:

MIBobject **.** *length-of-name* **.** *ASCII-value-for-each-character-in-name* **.** *type* **.** *number-of-octets-in-address* **.** *destination-address.destination-port*

The period (.) between each variable is required and a period (.) is also required between each character in the *ASCII-value-for-each-character-in-the-name argument*.

The following MIB string is for configuring an endpoint list (edgehosts-echo) with a destination IP address (10.1.1.1) and port (6500). See the table below for the appropriate values for each variable in the string

```
cipslaIPEndPointRowStatus.13.101.100.103.101.104.111.115.116.115.45.101.112.108.1.4.10.1.11.1.6500
 -i 4
```

Table 2: Values for MIB Strings to Configure an IP Address and Port in an Auto IP SLAs Endpoint List

Variable	Value	Comments
MIBobject	cipslaIPEndPointRowStatus	Creates an endpoint list.
length-of-template-nam e	13	To determine this value, count the number of characters in the name The name of this endpoint list in this example is: edgehosts-echo.
ASCII-value-for-each-character-in-name	101.100.103.101.104.111.115.116.115.45.101.112.108	To determine this value, replace each letter of the name with its ASCII equivalent. Each of the ASCII characters must be separated by a period (.). The name of this endpoint list in this example is: edgehosts-echo.
type	1	Type is: IP.
number- of-octets-in-address	4	IPv4 address (10.101.101.1) has four octets.
destination-address	10.1.1.1	Standard URL.
destination-port	6500	Port number.

Example MIB Strings for Auto IP SLAs Scheduler

This example shows the MIB strings for configuring a scheduler (theschedule) with an immediate start time.

The Cisco IOS commands for configuring a scheduler are:

- **ip sla auto schedule** *schedule-id*
- **start-time now**

The syntax for the MIB string to create a scheduler is as follows:

MIBobject **.** *length-of-name* **.** *ASCII-value-for-each-character-in-name*

The period (**.**) between each variable is required and a period (.) is also required between each character in the *ASCII-value-for-each-character-in-the-name* argument.

The following MIB strings are for configuring the scheduler (theschedule) in this example. See the table below for the appropriate values for each variable in the string.

- To create the scheduler, the MIB string is:

```
cipslaAutoGroupSchedRowStatus.11.116.104.101.115.99.104.101.100.117.108.101 -i 4
```

- To configure the start time in the schedule, the MIB string is

```
cipslaAutoGroupSchedStartTime.11.116.104.101.115.99.104.101.100.117.108.101 -g 0
```

Table 3: Values for MIB Strings to Configure an Auto IP SLAs Scheduler

Variable	Value	Comments
MIBobject	cipslaAutoGroupSchedRowStatus	Creates a scheduler.
	cipslaAutoGroupSchedStartTime	Configures start time.
length-of-nam e	11	To determine this value, count the number of characters in the name. The name of this scheduler in this example is: theschedule.
ASCII-value-for-each-character-in-name	116.104.101.115.99.104.101.100.117.108.101	To determine this value, replace each letter of the template name with its ASCII equivalent. Each of the ASCII characters must be separated by a period (.). The name of this template in this example is: theschedule.

Example MIB Strings for an Auto-Measure Group

This example shows the MIB strings for configuring an auto-measure group (customergroup).

The Cisco IOS commands for configuring a group are:

- **ip sla auto group type ip** *group-name*
- **template icmp-echo** *template-name*
- **destination** *template-name*
- **schedule** *schedule-id*

The syntax for the MIB string to configure a group is as follows:

MIBobject **.** *type* **.** *length-of-name* **.** *ASCII-value-for-each-character-in-name*

The period (**.**) between each variable is required and a period (.) is also required between each character in the *ASCII-value-for-each-character-in-the-name* argument.

Use the following MIB strings to configure the group (customergroup) in this example via SNMP. See the table below for the appropriate values for each variable in the string.

- To create the group, the MIB string is:

```
cipslaAutoGroupRowStatus.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -i 4 \
```

- To specify the template for this group, the MIB string is

```
cipslaAutoGroupOperType.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -i 1
cipslaAutoGroupOperTemplateName.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -D
"tml-icmpecho"
```

- To specify the endpoint list for this group, the MIB string is:

```
cipslaAutoGroupDestEndPointName.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -D
"edgehosts-epl"
```

- To specify a scheduler for this group, the MIB string is:

```
cipslaAutoGroupSchedulerId.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -D
"theschedule"
```

Table 4: Values for MIB Strings to Configure an IP SLAs Auto-Measure Group

Variable	Value	Comments
MIBobject	cipslaAutoGroupSchedRowStatus	Creates a group
	cipslaAutoGroupOperType	Defines operation type for group.
	cipslaAutoGroupOperTemplateName	Specifies a template.
	cipslaAutoGroupDestEndPointName	Specifies an endpoint list
	cipslaAutoGroupSchedulerId	Specifies a scheduler.
type	1	Type is: IP.
length-of-nam e	13	To determine this value, count the number of characters in the name. The name of this group in this example is: customergroup.

Variable	Value	Comments
ASCII-value-for-each-character-in-name	99.117.115.116.111.109.101.114.71.114.111.117.112	To determine this value, replace each letter of the template name with its ASCII equivalent. Each of the ASCII characters must be separated by a period (.). The name of this group in this example is: customergroup.

Example Using SNMP Commands to Create an Auto IP SLAs Operation

The following example shows how to use SNMP commands to create the configuration in the preceding examples using the setany application:

```
setany -v2c <ipaddress> public
cipslaIcmpEchoTmplStorageType.12.116.109.108.45.105.99.109.112.101.99.104.111 -i 3 \


               cipslaIcmpEchoTmplRowStatus.12.116.109.108.45.105.99.109.112.101.99.104.111
 -i 4



setany -v2c <ipaddress> public
cipslaIcmpEchoTmplTOS.12.116.109.108.45.105.99.109.112.101.99.104.111 -g 255



setany -v2c <ipaddress> public
cipslaIPEndPointRowStatus.13.101.100.103.101.104.111.115.116.115.45.101.112.108.1.4.10.1.1.1.6500
 -i 4 \



cipslaIPEndPointStorageType.13.101.100.103.101.104.111.115.116.115.45.101.112.108.1.4.10.1.1.1.6500
 -i 3



setany -v2c <ipaddress> public
cipslaAutoGroupSchedRowStatus.11.116.104.101.115.99.104.101.100.117.108.101 -i 4 \


cipslaAutoGroupSchedStorageType.11.116.104.101.115.99.104.101.100.117.108.101 -i 3



setany -v2c <ipaddress> public
cipslaAutoGroupSchedStartTime.11.116.104.101.115.99.104.101.100.117.108.101 -g 0



setany -v2c <ipaddress> public
cipslaAutoGroupRowStatus.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -i 4 \



cipslaAutoGroupStorageType.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -i 3



setany -v2c <ipaddress> public
```

```
cipslaAutoGroupSchedulerId.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -D
"theschedule"


setany -v2c <ipaddress> public
cipslaAutoGroupOperType.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -i 1 \


cipslaAutoGroupOperTemplateName.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -D
"tml-icmpecho"


setany -v2c <ipaddress> public
cipslaAutoGroupDestEndPointName.1.13.99.117.115.116.111.109.101.114.71.114.111.117.112 -D
"edgehosts-epl"
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
No new or modified standards or RFCs are supported by this feature, and support for existing standards has not been modified by features in this document.	--

MIBs

MIB	MIBs Link
• CISCO-IPSLA-VIDEO-MIB • CISCO-RTTMON-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

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

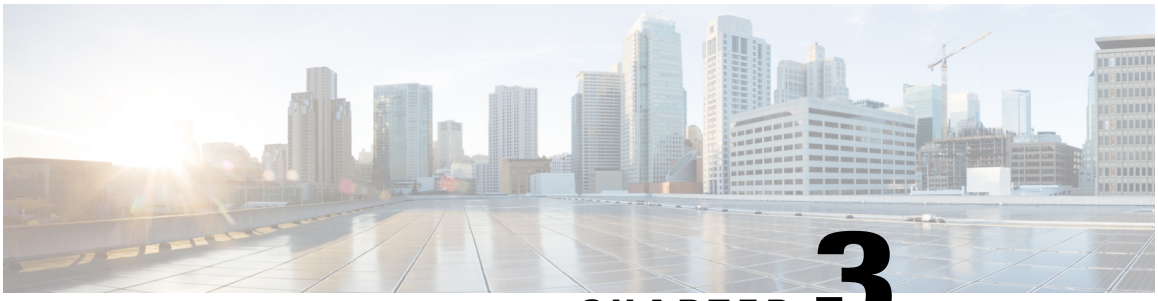
Feature Information for Auto IP SLAs in IP SLAs Engine 3.0

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 5: Feature Information for Auto IP SLAs in IP SLAs Engine 3.0

Feature Name	Releases	Feature Information
Cisco IOS IP SLAs Engine 3.0	15.1(1)T	Auto IP SLAs in Cisco IOS IP Service Level Agreements (SLAs) Engine 3.0 enables you to combine a template, endpoint list, and scheduler to easily configure multiple operations, including operations for proactive threshold monitoring, and provides auto registration which enables the source to discover the destination's address for building an endpoint list. The following commands were introduced or modified: **access-list**, **ageout**, **codec**(tplt), **clock-tolerance ntp oneway**, **description**(IP SLA), **control**, **destination**(am-group),**discover**(epl), **frequency**(am-schedule), **history buckets-kept**, **history distributions-of-statistics-kept**, **history enhanced**, **history filter**, **history hours-of-statistics-kept**, **history lives-kept**, **history statistics-distribution-interval**, **interval**(params), **ip-address** (epl), **ip sla auto discovery**, **ip sla auto endpoint-list**, **ip sla auto group**, **ip sla auto schedule**, **ip sla auto template**, **ip sla responder auto-register**,**life**, **measurement-retry**, **num-packets**, **operation-packet priority**, **parameters**, **precision**, **probe-interval**, **react**, **request-data-size**, **schedule**, **show ip sla auto discovery**, **show ip sla auto group**, **show ip sla auto summary-statistics**, **show ip sla auto schedule**, **show ip sla auto endpoint-list**, **show ip sla auto template**, **source-ip** (tplt), **source-port**, **start-time**, **template**(am-group), **threshold** (IP SLA), **tos**(IP SLA),**timeout**(IP SLA), **verify-data**(IP SLA), **vrf**(IP SLA).



CHAPTER 3

Configuring IP SLA - Percentile Support for Filtering Outliers

This module describes how to configure the percentile option for IP SLAs to examine a set of network measurements that are within a specified percentile of the return packets. This feature improves Cisco IP Service Level Agreements (SLAs) by providing the capability to measure round-trip times within a percentile, such as the 95th percentile of RTT, in order to examine a set of measurements that are 95% faster and 5% slower.

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.

Information About IP SLA - Percentile Support for Filtering Outliers

Percentile Measurements

The IP SLA- Percentile Support for Filtering Outliers feature enables IP SLAs to calculate min/average/max values for all packets, excluding those with the highest x% measured value. For example, if you have a ten-packet probe with nine 1-ms RTT values and one 50-ms RTT value, the percentile will exclude the outlier (50-ms) and report a min/avg/max value of 1/1/1, not 1/5/50.

IP SLAs reactions are configured to trigger when a monitored value exceeds or falls below a specified level. If IP SLAs measures too high or too low for any configured reaction, IP SLAs can generate a notification to a network management application or trigger another IP SLA operation to gather more data. The percentile reactions work the same way except that the monitored value is the percentile min/max/average. A count is keep of all the packets that violate the threshold value and at the end of the operation, that value is subtracted from the total packets received, then divided by the total, and a success ratio is generated. This value is referenced by a new reaction type that generates a notification when a percentage ratio is not met. For information, see the **ip sla reaction-configuration** command in the IP SLAs Command Reference.

How to Configure IP SLA - Percentile Support for Filtering Outliers

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** *ip-address* **port** *port***vrf** *vrf*
	
	Example:
	`Device(config)# ip sla responder`
	
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		(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.
		• Protocol control is enabled by default.

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

Configuring an IP SLAs Operation Using the Percentile Option

Before You Begin

- The IP SLAs operation to be configured for percentile support must be configured on the source device. For configuration information, see the appropriate module in the *IP SLAs Configuration Guide*. The percentile option can be configured for the following IP SLAs operations:
  - Ethernet jitter—See the "Manually Configuring an IP SLAs Ethernet Ping or Jitter Operation on the Source Device" section of the "Configuring IP SLAs for Metro-Ethernet" module.
  - ICMP jitter—See the "Configuring Cisco IP SLAs ICMP Operations" module.
  - UDP jitter—See the "IP SLAs UDP Jitter Operations" module.

- For a UDP jitter operation, an IP SLAs responder must be configured on the destination device. For configuration information, see the "Configuring an IP SLAs Responder on the Destination Device" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **percentile** {**jitteravg** | **jitterds** | **jittersd** | **owds** | **owsd** | **rtt**} *percent*
5. **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	**ip sla** *operation-number* **Example:** `Device(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode. **Note** For the purpose of this configuration task, the operation to be configured for percentile support is a preconfigured ICMP jitter operation.
Step 4	**percentile** {**jitteravg** | **jitterds** | **jittersd** | **owds** | **owsd** | **rtt**} *percent* **Example:** `Device(config-ip-sla-jitter)# percentile jitteravg 95`	Configures the percentile option for an IP SLAs operation.
Step 5	**end** **Example:** `Device(config-ip-sla-jitter)# end`	Returns to privileged EXEC mode.

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**]	• 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
	• **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*]}]	

	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`	

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 Operations

Perform this task to display and interpret the results of an IP SLAs operation. Check the output for fields that correspond to the criteria in your service level agreement to determine whether the service metrics are acceptable.

SUMMARY STEPS

1. **enable**
2. **show ip sla statistics**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show ip sla statistics**

Displays and interprets the results of an IP SLAs operation.

Example:

```
Device> show ip sla statistics
```

Configuration Examples for IP SLA - Percentile Support for Filtering Outliers

Example: Configuring IP SLA - Percentile Support for Filtering Outliers

The following example shows how to configure an IP SLAs ICMP jitter operation with the percentile option:

```
ip sla 1
 icmp-jitter 192.168.0.129 interval 40 num-packets 100 source-ip 10.1.2.34
 percentile jitteravg 95
!
ip sla reaction-configuration 1 react jitterAvgpct threshold-value 5 2 action-type trap
threshold-type immediate
!
ip sla schedule 1 start-time now life forever
```

Additional References for IP SLA - Percentile Support for Filtering Outliers

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 IP SLAs configuration tasks	*IP SLAs Configuration Guide*

Standards and RFCs

Standard/RFC	Title
• 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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

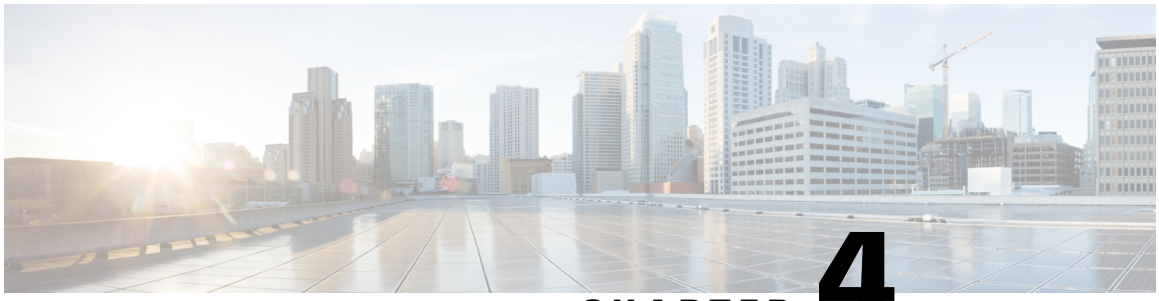
Feature Information for IP SLA - Percentile Support for Filtering Outliers

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 6: Feature Information for IP SLA - Percentile Support for Filtering Outliers

Feature Name	Releases	Feature Information
IP SLA - Percentile Support for Filtering Outliers	Cisco IOS 15.3(2)T	This feature improves Cisco IP Service Level Agreements (SLAs) by providing the capability to measure round-trip times within a percentile, such as the 95th percentile of RTT, in order to examine a set of measurements that are 95% faster and 5% slower. The following commands were introduced or modified: **ip sla reaction-configuration**, **percentile**, **show ip sla statistics**



CHAPTER 4

Configuring IP SLAs Video Operations

This document describes how to configure the Cisco IOS IP Service Level Agreements (SLAs) Video Operation feature to analyze one-way delay, one-way packet loss, one-way jitter, and connectivity in networks that carry video traffic.

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.

Prerequisites for IP SLAs Video Operations

- Both the source and responder devices for the IP SLAs video operation must be capable of providing platform-assisted video traffic generation and reflection.
- Time synchronization, such as that provided by Network Time Protocol (NTP), is required between the source and the responder device in order to provide accurate one-way delay (latency) measurements.

To configure NTP on the source and target devices, perform the tasks in the "Performing Basic System Management" module in the Cisco IOS Network Management Configuration Guide.

Restrictions for IP SLAs Video Operations

- This feature is supported only on Cisco devices that are capable of generating platform-assisted video traffic and reflection, such as the Cisco Catalyst 3560, 3560-E, 3560-X, 3750, 3750-E, and 3750-X Series switches.

Note The preceding list is not all inclusive. See your product documentation for more information.

- IP SLAs video operations do not support Round Trip Time (RTT) traffic.
- Because IP SLAs video operations support only one-way traffic, an operation and a responder must be configured on both the source and responder and both devices must support SNMP access.
- IP SLAs video operations are supported in IPv4 networks only.

Information About IP SLAs Video Operations

The platform-independent IP Service Level Agreements (SLAs) is a feature embedded in Cisco software. It allows you to understand IP service levels, increase productivity, lower operational costs, and reduce the frequency of network outages. IP SLAs performs the active monitoring of the network performance and can be used for network troubleshooting, network readiness assessment, and health monitoring.

IP SLAs in Cisco software is incapable of generating the high data rates, 4 to 16 Mbps, which are typical of video applications. To eliminate the protocol overhead and the process scheduling delays that contribute to the limitations of the earlier IP SLAs software to generate video traffic, the Cisco IP SLAs Video Operation feature makes the traffic generation and transmission routines platform dependent. The Application programming interface (API) calls in the IP SLAs video operation software to enable a more precise timer interrupt than the general system timer, which is insufficient for the packet generation requirements for a true video stream. Devices that can act as a source or a responder for an IP SLAs video operation are limited to Cisco devices that are capable of providing platform-assisted video traffic generation and reflection.

An IP SLAs video operation differs from other IP SLA operations in that all traffic is one way only, with a responder required to process the sequence numbers and time stamps locally and to wait for a request from the source before sending the calculated data back.

The source sends a request to the responder when the current video operation is done. This request signals the responder that no more packets will arrive, and that the video sink function in the video operation can be turned off. When the response from the responder arrives at the source, the statistics are read from the message, and the relevant fields in the operation are updated.

Because all video operation traffic is one way, the responder is responsible for actually collecting and verifying the packets. The software that does packet count verification and time stamp jitter calculations is shared by both the source and responder. The responder stores this information until such time that the source requests the data, or a timer expires and the data is released.

Because the responder cannot directly read the video packets, the responder creates two queues and a block of reallocated memory for use by both video sink and the responder itself.

When a packet arrives at video sink, it is processed to extract the sequence numbers and time stamps, and that information is put into one of the pre-allocated memory blocks. A pointer to this block is put into the used queue for later processing by the main responder task.

At periodic timer intervals, the responder processes a number of the packet information blocks from the used queue and updates the statistics appropriately. When the data is processed, the blocks are returned to the free-memory list to be used again.

This procedure continues until the video operation is complete.

How to Configure IP SLAs Video Operations

Configuring an IP SLAs Responder

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder**
4. **exit**

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 responder** **Example:** `Device(config-term)# ip sla responder`	Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-term)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IP SLAs Video Profile

To configure a source IP address for the operation and identify the prepackaged video profile to be used for the video traffic type to be analyzed, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **video** *destination-ip-address* | *destination-hostname destination-port* **source-ip** *source-address* | *source-hostname* **source-port** *port-number* **profile** *traffic-type*
5. **duration** *seconds*
6. **frequency** *seconds*
7. **history distribution-of-statistics-kept** *size*
8. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
9. **history hours-of-statistics-kept** *hours*
10. **history statistics-distribution-interval** *milliseconds*
11. **owner** *owner*
12. **tag** *text*
13. **timeout** *milliseconds*
14. **threshold** *milliseconds*
15. **vrf** *vrf-name*
16. **end**
17. **show ip sla configuration** [*operation-number*]

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** *operation-number* **Example:** `Device(config-term)# ip sla 10`	Begins configuration of an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**video** *destination-ip-address* | *destination-hostname* *destination-port* **source-ip** *source-address* | *source-hostname* **source-port** *port-number* **profile** *traffic-type* **Example:** `Device(config-ip-sla)# video 192.168.2.17 997 source-ip 192.168.2.16 source-port 555 profile telepresence`	Configures a source address and a prepackaged video profile for the IP SLAs operation being configured and enters IP SLA video configuration mode.
Step 5	**duration** *seconds* **Example:** `Device(config-ip-sla-video)# duration 20`	(Optional) Sets the amount of time during which synthetic traffic is generated for the IP SLAs video operation.
Step 6	**frequency** *seconds* **Example:** `Device(config-ip-sla-video)# frequency 60`	(Optional) Sets the amount of time during which synthetic traffic is generated for the IP SLAs video operation.
Step 7	**history distribution-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-video)# history distribution-of-statistics-kept 1`	(Optional) Sets the number of statistics distributions kept during the IP SLAs video operation.

	Command or Action	Purpose
Step 8	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Device(config-ip-sla-video)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for the IP SLAs video operation.
Step 9	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-video)# history hours-of-statistics-kept 2`	(Optional) Sets the number of hours for which statistics are maintained for the IP SLAs video operation.
Step 10	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-video)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for the IP SLAs video operation.
Step 11	**owner** *owner* **Example:** `Device(config-ip-sla-video)# 192.168.2.189 cwb.cisco.com User1 RTP 555-0100`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of the IP SLAs video operation.
Step 12	**tag** *text* **Example:** `Device(config-ip-sla-video)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for the IP SLAs video operation.
Step 13	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-video)# timeout 5000`	(Optional) Sets the amount of time the IP SLAs video operation waits for a response from its request packet.
Step 14	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-video)# threshold 5000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by the IP SLAs video operation.

	Command or Action	Purpose
Step 15	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-video)# vrf vpn-1`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) VPNs using IP SLAs operations.
Step 16	**end** **Example:** `Device(config-ip-sla-video)# end`	Returns to global configuration mode.
Step 17	**show ip sla configuration** [*operation-number*] **Example:** `Device# show ip sla configuration 600`	(Optional) Displays configuration information, including defaults, for all IP SLAs operations or a specified operation.

Configuring Proactive Threshold Monitoring

Perform this task to configure thresholds and reactive triggering for generating traps or starting another operation.

Before You Begin

- IP SLAs operations to be started when violation conditions are met must be configured.

Note

- RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).
- SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation. Only syslog messages are supported for RTTAvg threshold violations.
- Only syslog messages are supported for RTT violations during Jitter operations.
- Only SNMP traps are supported for RTT violations during non-Jitter operations.
- Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.
- Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]
4. **ip sla reaction-trigger** *operation-number target-operation*
5. **ip sla logging traps**
6. Do one of the following:
   - **snmp-server enable traps rtr**
   - **snmp-server enable traps syslog**
7. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
8. **exit**
9. **show ip sla reaction- configuration** [*operation-number*]
10. **show ip sla reaction- trigger** [*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 reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*] **Example:** `Device(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger`	Configures the action (SNMP trap or IP SLAs trigger) that is to occur based on violations of specified thresholds.
Step 4	**ip sla reaction-trigger** *operation-number target-operation* **Example:** `Device(config)# ip sla reaction-trigger 10 2`	(Optional) Starts another IP SLAs operation when the violation conditions are met. • Required only if the **ip sla reaction-configuration** command is configured with either the **trapAndTrigger**or **triggerOnly**keyword.
Step 5	**ip sla logging traps** **Example:** `Device(config)# ip sla logging traps`	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.

Step 6	Do one of the following:
	• **snmp-server enable traps rtr**
	• **snmp-server enable traps syslog**
	
	Example:
	`Device(config)# snmp-server enable traps rtr`
	
	Example:
	`Device(config)# snmp-server enable traps syslog`
		• (Optional) The first example shows how to enable the system to generate CISCO-RTTMON-MIB traps.
		• (Optional) The second example shows how to enable the system to generate CISCO-SYSLOG-MIB traps.

Step 7	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	(Optional) Sends traps to a remote host. • Required if the **snmp-server enable traps** command is configured.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server host 10.1.1.1 public syslog`	
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	**show ip sla reaction- configuration** [*operation-number*] **Example:** `Device# show ip sla reaction-configuration 10`	(Optional) Displays the configuration of proactive threshold monitoring.
Step 10	**show ip sla reaction- trigger** [*operation-number*] **Example:** `Device# show ip sla reaction-trigger 2`	(Optional) Displays the configuration status and operational state of target operations to be triggered.

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 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`	

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.

Displaying Statistics for IP SLAs

SUMMARY STEPS

1. **enable**
2. **show ip sla configuration** [*operation*]
3. **show ip sla statistics** [*operation-number*] [**details**]
4. **show ip sla statistics aggregated** [*operation-number*] [**details**]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip sla configuration** [*operation*] **Example:** `Device# show ip sla configuration 10`	(Optional) Displays configuration values, including all defaults, for all IP SLAs operations or the specified operation.
Step 3	**show ip sla statistics** [*operation-number*] [**details**] **Example:** `Device# show ip sla statistics 10 details`	(Optional) Displays display the current operational status and statistics of all IP SLAs operations or the specified operation.
Step 4	**show ip sla statistics aggregated** [*operation-number*] [**details**] **Example:** `Device# show ip sla statistics aggregated 10 deatils`	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or the specified operation.
Step 5	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

- If the IP SLAs operation is not running and not 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 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.

Configuration Examples for IP SLAs Video Operations

Example: Basic IP SLAs Video Profile for Cisco TelePresence 1080P Traffic

```
        IP SLAs Infrastructure Engine-III
Entry number: 600
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: video
Video profile name: TELEPRESENCE
Target address/Source address: 10.10.10.1/10.10.10.2
Target port/Source port: 1/1
Vrf Name:
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
```

Example: Basic IP SLAs Video Profile for IP Television Traffic

```
        IP SLAs Infrastructure Engine-III
Entry number: 700
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: video
Video profile name: IPTV
Target address/Source address: 10.10.10.3/10.10.10.4
Target port/Source port: 1/1
Vrf Name:
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
```

Example: Basic IP SLAs Video Profile for IP Surveillance Camera Traffic

```
        IP SLAs Infrastructure Engine-III
Entry number: 800
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: video
Video profile name: IPVSC
Target address/Source address: 10.10.10.5/10.10.10.6
Target port/Source port: 1/1
Vrf Name:
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
```

Example: SNMP Commands for Configuring a Video Operation

The following SNMP commands can be used to configure an IP SLAs video operation.

```
setany -v2c x.x.x.x public rttMonCtrlAdminStatus.1 -i 5 \ >
rttMonCtrlAdminRttType.1 -i 22 \ >
rttMonEchoAdminProtocol.1 -i 37 \ >
rttMonEchoAdminTargetPort.1 -i 7810 \ >
rttMonEchoAdminSourcePort.1 -i 7011 \ >
rttMonEchoAdminSourceAddress.1 -o "65 65 65 02" \ >
rttMonEchoAdminVideoTrafficProfile.1 -o "IPTV" \ >
rttMonCtrlAdminNvgen.1 -i true \ >
rttMonEchoAdminTargetAddress.1 -o "65 65 65 01"
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
No new or modified standards or RFCs are supported by this feature, and support for existing standards has not been modified by features in this document.	--

MIBs

MIB	MIBs Link
• CISCO-IPSLA-VIDEO-MIB • CISCO-RTTMON-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

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

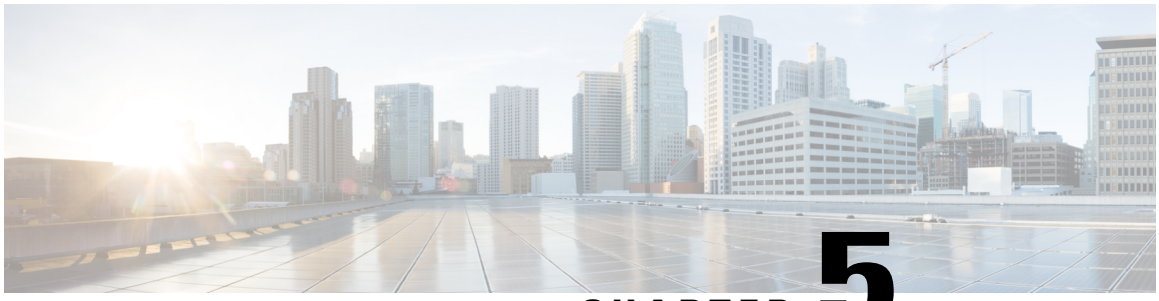
Feature Information for IP SLAs Video Operations

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 7: Feature Information for IP SLAs Video Operations

Feature Name	Releases	Feature Information
IP SLAs Video Operations	12.2(58)SE 15.2(2)T 15.1(1)SG Cisco IOS XE Release 3.3SG	Analyzes one-way delay, one-way packet loss, one-way jitter, and connectivity in IPv4 networks that carry video traffic. The following commands were introduced or modifed: **bitrate**, **codec (VO profile)**, **description (VO profile)**, **dscp (IP SLA video)**, **endpoint**, **frame (VO profile)**, **ip sla profile video**, **reserve dsp**, **resolution**, **rtp (VO profile)**, **show ip sla video**, **video (IP SLA)**, **video content**.



CHAPTER 5

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.

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.

Restrictions for IP SLAs UDP Jitter Operations

- Multiple SLA probes configured with same source and destination IP and port number must not be run simultaneously.

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 8: 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***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** *ip-address* **port** *port***vrf** *vrf*
	
	Example:
	`Device(config)# ip sla responder`
	
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		(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.
		• 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 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`	

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**
4. **show ip sla statistics**
5. **show ip sla statistics 2 details**

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
```

Step 4 **show ip sla statistics**
Displays IP SLAs statistics.

Example:

```
Device# show ip sla statistics

Type of operation: udp-jitter
Packet Loss Values:
Loss Source to Destination: 19
Source to Destination Loss Periods Number: 19
Source to Destination Loss Period Length Min/Max: 1/1
Source to Destination Inter Loss Period Length Min/Max: 1/546
Loss Destination to Source: 0
Destination to Source Loss Periods Number: 0
Destination to Source Loss Period Length Min/Max: 0/0
Destination to Source Inter Loss Period Length Min/Max: 0/0
Out Of Sequence: 0 Tail Drop: 0
Packet Late Arrival: 0 Packet Skipped: 0
```

- udp-jitter has the ability to detect in which direction a packet was lost in. It also calculates statistics about the periods of packet loss
- Loss Source to Destination: 19—Indicates that 19 packets were sent from the sender but never reached the responder.
- Source to Destination Loss Periods Number: 19—Indicates that there were 19 incidents of packet loss (an incident of packet loss is a period where packets are lost, irrespective of the actual number of lost packets.)
- Source to Destination Loss Period Length Min/Max: 1/1—indicates that all packets lost in this direction are isolated; there are no instances of multiple lost packets back-to-back.
- Source to Destination Inter Loss Period Length Min/Max: 1/546—indicates that the minimum gap between lost packets is 1, and the maximum gap between successive packet losses is 546 successfully sent packets.

Step 5 **show ip sla statistics 2 details**
Displays IPSLAs latest operation statistics

Example:

```
Device# show ip sla statistics 2 details

IPSLA operation id: 2
Type of operation: udp-jitter
Latest RTT: 1 milliseconds
Latest operation start time: 07:45:28 GMT Thu Aug 28 2014
Latest operation return code: OK
Over thresholds occurred: FALSE
RTT Values:
Number Of RTT: 10 RTT Min/Avg/Max: 1/1/1 milliseconds
Latency one-way time:
Number of Latency one-way Samples: 6
Source to Destination Latency one way Min/Avg/Max: 1/1/1 milliseconds
Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Source to Destination Latency one way Sum/Sum2: 6/6
Destination to Source Latency one way Sum/Sum2: 0/0
Jitter Time:
Number of SD Jitter Samples: 9
Number of DS Jitter Samples: 9
Source to Destination Jitter Min/Avg/Max: 0/1/1 milliseconds
Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Source to destination positive jitter Min/Avg/Max: 1/1/1 milliseconds
Source to destination positive jitter Number/Sum/Sum2: 3/3/3
Source to destination negative jitter Min/Avg/Max: 1/1/1 milliseconds
Source to destination negative jitter Number/Sum/Sum2: 3/3/3
Destination to Source positive jitter Min/Avg/Max: 0/0/0 milliseconds
Destination to Source positive jitter Number/Sum/Sum2: 0/0/0
Destination to Source negative jitter Min/Avg/Max: 0/0/0 milliseconds
Destination to Source negative jitter Number/Sum/Sum2: 0/0/0
Interarrival jitterout: 0 Interarrival jitterin: 0
Jitter AVG: 1
Over Threshold:
Number Of RTT Over Threshold: 0 (0%)
Packet Loss Values:
Loss Source to Destination: 0
Source to Destination Loss Periods Number: 0
Source to Destination Loss Period Length Min/Max: 0/0
Source to Destination Inter Loss Period Length Min/Max: 0/0
Loss Destination to Source: 0
Destination to Source Loss Periods Number: 0
Destination to Source Loss Period Length Min/Max: 0/0
Destination to Source Inter Loss Period Length Min/Max: 0/0
Out Of Sequence: 0 Tail Drop: 0 Packet Late Arrival: 0
Packet Skipped: 0
Voice Score Values:
Calculated Planning Impairment Factor (ICPIF): 0
Mean Opinion Score (MOS): 0
Number of successes: 2
Number of failures: 0
Operation time to live: Forever
Operational state of entry: Active
Last time this entry was reset: 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

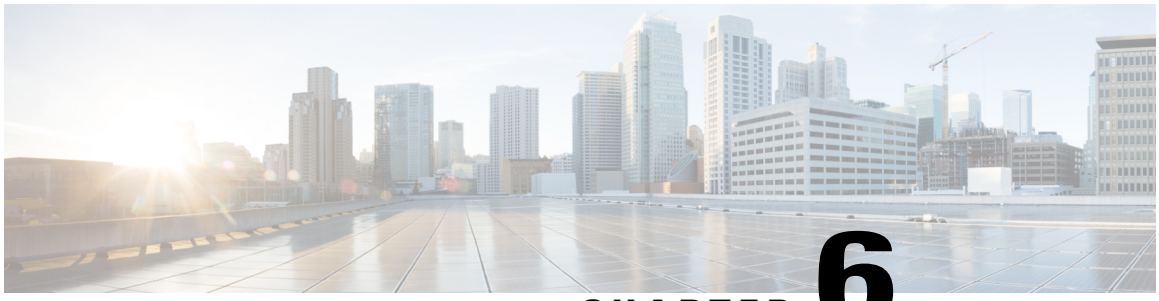
Technical Assistance

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 9: 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.
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**.



CHAPTER 6

IP SLA - Support for OnDemand UDP Probes

This module describes how to configure an IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) probe to enable real-time network troubleshooting for users without configuration privileges. This feature supports on-demand UDP operations that can be run by issuing a single command in privileged EXEC mode.

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.

Information About IP SLA - Support for OnDemand UDP Probes

OnDemand UDP Probes

A single command in privileged EXEC mode can be used to specify frame size, interval, frequency, and duration for an on-demand IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) operation. Configuring the command creates two IP SLAs operations. The first operation is a generic IP SLA operation that acts as a shell to handle events, timers, and the parser action functions. The generic operation exists for

the single run of the exec command. A second temporary operation is created of the type requested by the user. The second operation performs the packet generation and statistic calculations. When the second operation is finished running, it sends an event to the generic operation. The generic operation then calls the print functions of the second operation. After the statistics are displayed, or after either a timeout occurs or the user issues a **clear** command, both operations are deleted.

How to Configure IP SLA - Support for OnDemand UDP Probes

Configuring an IP SLAs Responder on the Destination Device

Before You Begin

The networking device to be used as the responder must be a Cisco device and you must have connectivity to that device through the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder**
4. **exit**

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 responder** **Example:** `Device(config)# ip sla responder`	Temporarily enables IP SLAs responder functionality on a Cisco device in response to control messages from the source. • Control is enabled by default.
Step 4	**exit** **Example:** `Device(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring an OnDemand UDP Probe

Before You Begin

An IP SLAs responder must be configured on the destination device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**interval** *number*] [**num-packets** *packet-number*] [**optimize timestamp**] [**precision** {**microseconds** | **milliseconds**}] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *source-port*] [**tos** *number* | **traffic-class** *number*] [**vrf** *vrf-name*]

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 udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**interval** *number*] [**num-packets** *packet-number*] [**optimize timestamp**] [**precision** {**microseconds** | **milliseconds**}] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *source-port*] [**tos** *number* | **traffic-class** *number*] [**vrf** *vrf-name*]
	
	Example:
	`Device(config)# ip sla udp-jitter 2001:DB8:1::1 1000 num-packets 6000`
	`Device(config)# ip sla udp-jitter 192.168.2.1 5001 num-packets 6000`
		Creates and starts an on-demand UDP jitter operation.
		Note This step includes sample commands using IPv4 and IPv6 destination IP addresses.

Configuring an OnDemand UDP Probe for VoIP

Before You Begin

An IP SLAs responder must be configured on the destination device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **codec** *codec-type* [**advantage-factor** *value*] [**codec-interval** *milliseconds*] [**codec-numpackets** *packet-number*] [**codec-size** *number-of-bytes*] [**optimize timestamp**] [**precision** {**microseconds** | **milliseconds**}] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *source-port*] [**tos** *number* | **traffic-class** *number*] [**vrf** *vrf-name*]

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 udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **codec** *codec-type* [**advantage-factor** *value*] [**codec-interval** *milliseconds*] [**codec-numpackets** *packet-number*] [**codec-size** *number-of-bytes*] [**optimize timestamp**] [**precision** {**microseconds** | **milliseconds**}] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *source-port*] [**tos** *number* | **traffic-class** *number*] [**vrf** *vrf-name*]
	
	Example:
	`Device(config)# ip sla udp-jitter 2001:DB8:1::1 1000 codec g711ulaw`
	
	`Device(config)# ip sla udp-jitter 192.168.2.1 1000 codec g711ulaw`
		Creates and starts an on-demand UDP-based VoIP operation.
		Note This step includes sample commands using IPv4 and IPv6 destination IP addresses.

Configuring an OnDemand UDP Echo Probe

Before You Begin

An IP SLAs responder is optional for an on-demand UDP echo operation. We recommend using a Cisco networking device as the destination device, although any networking device that supports RFC 862, *Echo Protocol*, can be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**flow-label** *number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *source-port*] [**tos** *number* | **traffic-class** *number*] [**vrf** *vrf-name*]

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 udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**flow-label** *number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *source-port*] [**tos** *number* | **traffic-class** *number*] [**vrf** *vrf-name*]
	
	Example:
	`Device(config)# ip sla udp-echo 2001:DB8:1::1 1000`
	`Device(config)# ip sla udp-echo 192.168.2.1 1000`
		Creates and starts an on-demand UDP echo operation.
		Note This step includes sample commands using IPv4 and IPv6 destination IP addresses.

Configuration Examples for IP SLA - Support for OnDemand UDP Probes

Example: OnDemand UDP Jitter Probe

Issuing the **ip-sla udp jitter** command creates a temporary operation that performs packet generation and statistic calculations. After the statistics are displayed, the operation is deleted.

```
Device# ip sla udp-jitter 192.168.2.1 5001 num-packets 6000

Type of operation: udp-jitter
        Latest RTT: 1 milliseconds
Latest operation start time: 11:21:55 PDT Thu May 10 2012 Latest operation return code: OK
 RTT Values:
        Number Of RTT: 6000             RTT Min/Avg/Max: 1/1/2 milliseconds
Latency one-way time:
```

```
        Number of Latency one-way Samples: 6000
        Source to Destination Latency one way Min/Avg/Max: 1/0/2 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 0/0/1 milliseconds Jitter Time:
        Number of SD Jitter Samples: 5999
        Number of DS Jitter Samples: 5999
        Source to Destination Jitter Min/Avg/Max: 0/1/1 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/1/1 milliseconds Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0 Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 1
Number of failures: 0
```

Additional References for IP SLA - Support for OnDemand UDP Probes

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 862	*Echo Protocol*

MIBs

MIB	MIBs Link
• CISCO-RTTMON-MIB • IPV6-FLOW-LABEL-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

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

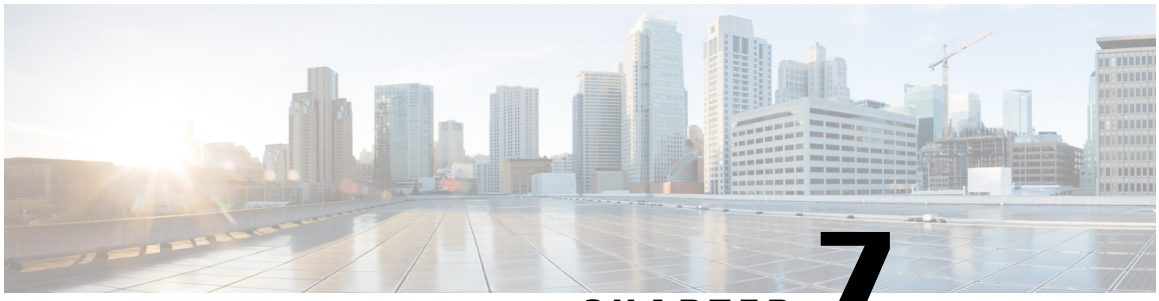
Feature Information for IP SLA - Support for OnDemand UDP Probes

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 10: Feature Information for IP SLA - Support for OnDemand UDP Probes

Feature Name	Releases	Feature Information
IP SLA - Support for OnDemand UDP Probes	15.3(1)T	Enables users without configuration privileges to create and run an IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) probe for real-time network troubleshooting. The following commands were introduced or modified: **ip sla udp-echo**, **ip sla udp-jitter**, **ip sla udp-jitter codec**.



CHAPTER 7

Configuring IP SLAs UDP Jitter Operations for VoIP

This document describes how to configure an IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation to proactively monitor Voice over IP (VoIP) quality levels in your network, allowing you to guarantee VoIP quality levels to your users in IPv4 or IPv6 networks. The IP SLAs VoIP UDP jitter operation accurately simulates VoIP traffic using common codecs and calculates consistent voice quality scores (MOS and ICPIF) between Cisco devices in the network.

Note The term "Voice" in this document should be taken to mean any Internet telephony applications. The term "Voice over IP" can include the transmission of multimedia (both voice and video) over IP networks.

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 Jitter Operations for VoIP

- This feature uses UDP traffic to generate approximate Voice over IP scores. It does not provide support for the Real-Time Transport Protocol (RTP).
- ICPIF and MOS values provided by this feature, while consistent within IP SLAs, are estimates only and are intended only for relative comparisons. The values may not match values determined using other methods.
- Predictions of customer opinion (such as those listed for the E-Model transmission rating factor R and derived Mean Opinion Scores) determined by any method are intended only for transmission planning and analysis purposes and should not be interpreted as reflecting actual customer opinions.

Information About IP SLAs UDP Jitter Operations for VoIP

The Calculated Planning Impairment Factor (ICPIF)

The ICPIF originated in the 1996 version of ITU-T recommendation G.113, "Transmission impairments," as part of the formula *Icpif = Itot - A*. ICPIF is actually an acronym for "(Impairment) Calculated Planning Impairment Factor," but should be taken to simply mean the "calculated planning impairment factor." The ICPIF attempts to quantify, for comparison and planning purposes, the key impairments to voice quality that are encountered in the network.

The ICPIF is the sum of measured impairment factors (total impairments, or *Itot*) minus a user-defined access Advantage Factor (*A*) that is intended to represent the user's expectations, based on how the call was placed (for example, a mobile call versus a land-line call). In its expanded form, the full formula is expressed as:

Icpif = Io + Iq + Idte + Idd + Ie - A

where

- *Io* represents impairments caused by non-optimal loudness rating,
- *Iq* represents impairments caused by PCM quantizing distortion,
- *Idte* represents impairments caused by talker echo,
- *Idd* represents impairments caused by one-way transmission times (one-way delay),
- *Ie* represents impairments caused by equipment effects, such as the type of codec used for the call and packet loss, and
- *A* represents an access Advantage Factor (also called the user Expectation Factor) that compensates for the fact that users may accept some degradation in quality in return for ease of access.

ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically less than 20 are generally considered "adequate." While intended to be an objective measure of voice quality, the ICPIF value is also used to predict the subjective effect of combinations of impairments. The table below, taken from G.113 (02/96), shows how sample ICPIF values are expected to correspond to subjective quality judgement.

Table 11: Quality Levels as a Function of Total Impairment Factor ICPIF

Upper Limit for ICPIF	Speech Communication Quality
5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

For further details on the ICPIF, see the 1996 version of the G.113 specification.

Note The latest version of the ITU-T G.113 Recommendation (2001), no longer includes the ICPIF model. Instead, it refers implementers to G.107: "The Impairment Factor method, used by the E-model of ITU-T G.107, is now recommended. The earlier method that used Quantization Distortion Units is no longer recommended." The full E-Model (also called the ITU-T Transmission Rating Model), expressed as $R = Ro - Is - Id - Ie + A$, provides the potential for more accurate measurements of call quality by refining the definitions of impairment factors (see the 2003 version of the G.107 for details). Though the ICPIF shares terms for impairments with the E-Model, the two models should not be confused. The IP SLAs VoIP UDP Operation feature takes advantage of observed correspondences between the ICPIF, transmission rating factor R, and MOS values, but does not yet support the E-Model.

IP SLAs uses a simplified ICPIF formula, defined in more detail later in this document.

Mean Opinion Scores (MOS)

The quality of transmitted speech is a subjective response of the listener. Each codec used for transmission of Voice over IP provides a certain level of quality. A common benchmark used to determine the quality of sound produced by specific codecs is MOS. With MOS, a wide range of listeners have judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The opinion scores are averaged to provide the mean for each sample. The table below shows MOS ratings and the corresponding description of quality for each value.

Table 12: MOS Ratings

Score	Quality	Description of Quality Impairment
5	Excellent	Imperceptible
4	Good	Just perceptible, but not annoying

Score	Quality	Description of Quality Impairment
3	Fair	Perceptible and slightly annoying
2	Poor	Annoying but not objectionable
1	Bad	Very annoying and objectionable

As the MOS ratings for codecs and other transmission impairments are known, an estimated MOS can be computed and displayed based on measured impairments. This estimated value is designated as MOS-CQE (Mean Opinion Score; Conversational Quality, Estimated) by the ITU in order to distinguish it from objective or subjective MOS values (see *P.800.1 Mean Opinion Score (MOS) terminology - ITU* for details).

Voice Performance Monitoring Using IP SLAs

One of the key metrics in measuring voice and video quality over an IP network is jitter. Jitter is the name used to indicate the variation in delay between arriving packets (inter-packet delay variance). Jitter affects voice quality by causing uneven gaps in the speech pattern of the person talking. Other key performance parameters for voice and video transmission over IP networks include latency (delay) and packet loss. IP SLAs is an embedded active monitoring feature of Cisco software that provides a means for simulating and measuring these parameters in order to ensure your network is meeting or exceeding service-level agreements with your users.

IP SLAs provides a UDP jitter operation, which consists of UDP probe packets sent across the network from an origin device to a specific destination (called the operational target). This synthetic traffic is used to record the amount of jitter for the connection, as well as the round-trip time, per-direction packet loss, and one-way delay time (one-way latency). The term “synthetic traffic” indicates that the network traffic is simulated; that is, the traffic is generated by IP SLAs. Data, in the form of collected statistics, can be displayed for multiple tests over a user-defined period of time, allowing you to see, for example, how the network performs at different times of the day, or over the course of a week. The jitter probe has the advantage of utilizing the IP SLAs Responder to provide minimal latency at the receiving end.

The IP SLAs VoIP UDP jitter operation modifies the standard UDP jitter operation by adding the capability to return MOS and ICPIF scores in the data collected by the operation, in addition to the metrics already gathered by the UDP jitter operation. This VoIP-specific implementation provides even more useful information in determining the performance of your VoIP network, thereby improving your ability to perform network assessment, troubleshooting, and health monitoring.

Codec Simulation Within IP SLAs

The IP SLAs VoIP UDP jitter operation computes statistics by sending n UDP packets, each of size s, sent t milliseconds apart, from a given source device to a given target device, at a given frequency f. The target device must be running the Cisco IP SLAs Responder in order to process the probe operations.

To generate MOS and ICPIF scores, you must specify the codec type used for the connection when configuring the VoIP UDP jitter operation. Based on the type of codec you configure for the operation, the number of packets (n), the size of each payload (s), the inter-packet time interval (t), and the operational frequency (f) will be auto-configured with default values. However, you are given the option, if needed, to manually configure these parameters in the syntax of the**udp-jitter** command.

The table below shows the default parameters that are configured for the operation by codec.

Table 13: Default VoIP UDP Jitter Operation Parameters by Codec

Codec	Default Request Size (Packet Payload) (s)	Default Interval Between Packets (t)	Default Number of Packets (n)	Frequency of Probe Operations (f)
G.711 mu-Law (g711ulaw)	160 + 12 RTP bytes	20 ms	1000	Once every 1 minute
G.711 A-Law (g711alaw)	160 + 12 RTP bytes	20 ms	1000	Once every 1 minute
G.729A (g729a)	20 + 12 RTP bytes	20 ms	1000	Once every 1 minute

For example, if you configure the VoIP UDP jitter operation to use the characteristics for the g711ulaw codec, by default a probe operation will be sent once a minute (**f**). Each probe operation would consist of 1000 packets (**n**), with each packet containing 180 bytes of synthetic data (**s**), sent 20 milliseconds apart (**t**).

The IP SLAs ICPIF Value

ICPIF value computation with Cisco software is based primarily on the two main factors that can impair voice quality: delayed packets and lost packets. Because packet delay and packet loss can be measured by IP SLAs, the full ICPIF formula, *Icpif = Io + Iq + Idte + Idd + Ie - A*, is simplified by assuming the values of *Io* , *Iq* , and *Idte* are zero, resulting in the following formula:

Total Impairment Factor (Icpif) = Delay Impairment Factor (Idd) + Equipment Impairment Factor (Ie) - Expectation/Advantage Factor (A)

This means that the ICPIF value is computed by adding a Delay Impairment Factor, which is based on a measurement of delayed packets, and an Equipment Impairment Factor, which is based on a measurement of lost packets. From this sum of the total impairments measured in the network, an impairment variable (the Expectation Factor) is subtracted to yield the ICPIF.

This is the same formula used by Cisco Gateways to calculate the ICPIF for received VoIP data streams.

The Delay Impairment Factor

The Delay Impairment Factor (*Idd*) is a number based on two values. One value is fixed and is derived using the static values (as defined in the ITU standards) for Codec Delay, Look Ahead Delay, and Digital Signal Processing (DSP) Delay. The second value is variable and is based on the measured one-way delay (round-trip time measurement divided by 2). The one-way delay value is mapped to a number using a mapping table that is based on a G.107 (2002 version) analytic expression. The table below shows sample correspondences between the one-way delay measured by IP SLAs and Delay Impairment Factor values.

Table 14: Sample Correspondence of One-Way Delay to ICPIF Delay Impairment

One-Way Delay (ms)	Delay Impairment Factor
50	1
100	2
150	4
200	7

The Equipment Impairment Factor

The Equipment Impairment Factor (*Ie*) is a number based on the amount of measured packet loss. The amount of measured packet loss, expressed as a percentage of total number of packets sent, corresponds an Equipment Impairment Factor that is defined by codec. The table below shows sample correspondences between the packet loss measured by IP SLAs and Equipment Impairment Factor values.

Table 15: Sample Correspondence of Measured Packet Loss to ICPIF Equipment Impairment

Packet Loss (as a percentage of total number of packets sent)	Equipment Impairment Value for PCM (G.711) Codecs	Equipment Impairment Value for the CS-ACELP (G.729A) Codec
2%	12	20
4%	22	30
6%	28	38
8%	32	42

The Expectation Factor

The Expectation Factor, also called the Advantage Factor (*A*), is intended to represent the fact that users may accept some degradation in quality in return for ease of access. For example, a mobile phone user in a hard-to-reach location may have an expectation that the connection quality will not be as good as a traditional land-line connection. This variable is also called the Advantage Factor (short for Access Advantage Factor) because it attempts to balance an increased access advantage against a decline in voice quality.

The table below, adapted from ITU-T Rec. G.113, defines a set of provisional maximum values for *A* in terms of the service provided.

Table 16: Advantage Factor Recommended Maximum Values

Communication Service	Advantage / Expectation Factor: Maximum value of A
Conventional wire-line (land-line)	0

Communication Service	Advantage / Expectation Factor: Maximum value of A
Mobility (cellular connections) within a building	5
Mobility within a Geographical area or moving in a vehicle	10
Access to hard-to-reach location; (for example, via multi-hop satellite connections)	20

These values are only suggestions. To be meaningful, the use of the factor *A* and its selected value in a specific application should be used consistently in any planning model you adopt. However, the values in the table above should be considered as the absolute upper limits for *A* .

The default Advantage Factor for IP SLAs VoIP UDP jitter operations is always zero.

The IP SLAs MOS Value

IP SLAs uses an observed correspondence between ICPIF and MOS values to estimate an MOS value. Usage of the abbreviation MOS within the context of this feature should be taken to represent the MOS-CQE (Mean Opinion Score; Conversational Quality, Estimated).

The E model, as defined in G.107 (03/2003), predicts the subjective quality that is experienced by an average listener by combining the impairment caused by transmission parameters (such as loss and delay) into a single rating, the transmission rating factor R (the R Factor). This rating, expressed in a scale of 0 (worst) to 100 (best) can be used to predict subjective user reactions, such as the MOS. Specifically, the MOS can be obtained from the R Factor with a converting formula. Conversely, a modified inverted form can be used to calculate R Factors from MOS values.

There is also a relationship between the ICPIF value and the R Factor. IP SLAs takes advantage of this correspondence by deriving the approximate MOS score from an estimated R Factor, which, in turn, is derived from the ICPIF score. The table below shows the resulting MOS values that will be generated for corresponding ICPIF values.

Table 17: Correspondence of ICPIF Values to MOS Values

ICPIF Range	MOS	Quality Category
0 - 3	5	Best
4 - 13	4	High
14 - 23	3	Medium
24 - 33	2	Low
34 - 43	1	Poor

IP SLAs will always express the estimated MOS value as a number in the range of 1 to 5, with 5 being the best quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.

How to Configure IP SLAs UDP Jitter Operations for VoIP

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** *ip-address* **port** *port***vrf** *vrf*	(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:
	`Device(config)# ip sla responder`
	
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		• 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 an IP SLAs VoIP UDP Jitter Operation

Note

- Currently, IP SLAs supports only the following speech codecs (compression methods):
  - G.711 A Law (g711alaw: 64 kbps PCM compression method)
  - G.711 mu Law (g711ulaw: 64 kbps PCM compression method)
  - G.729A (g729a: 8 kbps CS-ACELP compression method)
- The following commands, available in UDP jitter configuration mode, are not valid for UDP jitter (codec) operations:
  - **history distributions-of-statistics-kept**
  - **history statistics-distribution-interval**
  - **request-data-size**
- Specifying the codec-type will configure the appropriate default values for the **codec-interval**, **codec-size**, and **codec-numpacket** options. You should not specify values for the interval, size, and number of packet options unless you have a specific reason to override the defaults (for example, approximating a different codec).
- The **show ip sla configuration** command will list the values for the "Number of statistic distribution buckets kept" and "Statistic distribution interval (milliseconds)," but these values do not apply to jitter (codec) operations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **codec** *codec-type* [**codec-numpackets** *number-of-packets*] [**codec-size** *number-of-bytes*] [**codec-interval** *milliseconds*] [**advantage-factor** *value*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
6. **frequency** *seconds*
7. **history hours-of-statistics-kept** *hours*
8. **owner** *owner-id*
9. **tag** *text*
10. **threshold** *milliseconds*
11. **timeout** *milliseconds*
12. Do one of the following:
    - **tos** *number*
    - **traffic-class** *number*
13. **flow-label** *number*
14. **verify-data**
15. **vrf** *vrf-name*
16. **end**
17. **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.

	Command or Action	Purpose
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* **codec** *codec-type* [**codec-numpackets** *number-of-packets*] [**codec-size** *number-of-bytes*] [**codec-interval** *milliseconds*] [**advantage-factor** *value*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] **Example:** `Device(config-ip-sla)# udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 10`	Configures the operation as a jitter (codec) operation that will generate VoIP scores in addition to latency, jitter, and packet loss statistics.
Step 5	**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 6	**frequency** *seconds* **Example:** `Device(config-ip-sla-jitter)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 7	**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.
Step 8	**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 9	**tag** *text* **Example:** `Device(config-ip-sla-jitter)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 10	**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 11	**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 12	Do one of the following:
	• **tos** *number*
	• **traffic-class** *number*
	Example:
	`Device(config-ip-sla-jitter)# tos 160`
	Example:
	`Device(config-ip-sla-jitter)# traffic-class 160`
		(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 13	**flow-label** *number* **Example:** `Device(config-ip-sla-jitter)# flow-label 112233`	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 14	**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 15	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-jitter)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 16	**end** **Example:** `Device(config-ip-sla-jitter)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 17	**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.

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** *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*]}]
	
	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 Jitter Operations for VoIP

Example IP SLAs VoIP UDP Operation Configuration

The following example assumes that the Cisco IP SLAs Responder is enabled on the device at 209.165.200.225.

```
Device> enable

Password:
Device# configure terminal

Enter configuration commands, one per line.  End with the end command.
Device(config)# ip sla 10
Device(config-sla)# udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 2

Device(config-sla-jitter)# owner admin_bofh
Device(config-sla-jitter)# exit

Device(config)# ip sla schedule 10 start-time now

Device(config)# exit

Device#
Device# show running-config | begin ip sla 10

ip sla 10
 udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 2
 owner admin_bofh
ip sla schedule 10 start-time now
 .
 .
 .
Device# show ip sla configuration 10

Entry number: 10
Owner: admin_bofh
```

```
Tag:
Type of operation to perform: jitter
Target address: 209.165.200.225
Source address: 0.0.0.0
Target port: 16384
Source port: 0
Operation timeout (milliseconds): 5000
Codec Type: g711alaw
Codec Number Of Packets: 1000
Codec Packet Size: 172
Codec Interval (milliseconds): 20
Advantage Factor: 2
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 3600
Entry Ageout (seconds): never
Status of entry (SNMP RowStatus): Active
Connection loss reaction enabled: No
Timeout reaction enabled: No
Verify error enabled: No
Threshold reaction type: Never
Threshold (milliseconds): 5000
Threshold Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Reaction Type: None
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
```

When a codec type is configured for a jitter operation, the standard jitter "Request size (ARR data portion)," "Number of packets," and "Interval (milliseconds)" parameters will not be displayed in the **show ip sla configuration** command output. Instead, values for "Codec Packet Size," "Codec Number of Packets," and "Codec Interval (milliseconds)" are displayed.

Example IP SLAs VoIP UDP Operation Statistics Output

Use the **show ip sla statistics** command to display Voice scores (ICPIF and MOS values) for the jitter (codec) operation.

```
Device# show ip sla statistics 10

Entry number: 10
Modification time: 12:57:45.690 UTC Sun Oct 26 2003
Number of operations attempted: 1
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 19
Latest operation start time: 12:57:45.723 Sun Oct 26 2003
Latest operation return code: OK
!
Voice Scores:
ICPIF:  20          MOS Score:  3.20
!
RTT Values:
NumOfRTT: 10     RTTAvg: 19      RTTMin: 19     RTTMax: 20
RTTSum:  191    RTTSum2: 3649
Packet Loss Values:
```

```
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0
Jitter Values:
NumOfJitterSamples: 9
MinOfPositivesSD: 0     MaxOfPositivesSD: 0
NumOfPositivesSD: 0     SumOfPositivesSD: 0     Sum2PositivesSD: 0
MinOfNegativesSD: 0     MaxOfNegativesSD: 0
NumOfNegativesSD: 0     SumOfNegativesSD: 0     Sum2NegativesSD: 0
MinOfPositivesDS: 1     MaxOfPositivesDS: 1
NumOfPositivesDS: 1     SumOfPositivesDS: 1     Sum2PositivesDS: 1
MinOfNegativesDS: 1     MaxOfNegativesDS: 1
NumOfNegativesDS: 1     SumOfNegativesDS: 1     Sum2NegativesDS: 1
Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
NumOfOW: 0
OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0
```

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
Voice over IP (VoIP) codecs	Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation
Jitter in Packet Voice Networks	Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms) shtml

Standards and RFCs

Standard[1]/RFC[2]	Title
ITU-T Recommendation G.107 (2003)	The E-model, a computation model for use in transmission planning
ITU-T Recommendation G.113 (1996)	*Transmission impairments*
ITU-T Recommendation G.113 (2001)	Transmission impairments due to speech processing
ITU-T Recommendation G.711 (1998)	*Pulse code modulation (PCM) of voice frequencies* (also known as the G.711 Voice Codec)
ITU-T Recommendation G.729 Annex A (1996)	*Reduced complexity 8 kbit/s CS-ACELP speech codec* (also known as the G.729/A/B Speech Codec)
ITU-T Recommendation P.800.1 (2003)	Mean Opinion Score (MOS) terminology

Standard[1]/RFC[2]	Title
RFC 768	*User Datagram Protocol*
RFC 1889	*RTP: A Transport Protocol for Real-Time Applications*

1 Full support by this feature for listed RFCs is not claimed. ITU Telecommunication Standards ("ITU-T Recommendations In Force") can be obtained from http://www.itu.ch. Summary definitions are available from a variety of internet sources.
2 Full support by this feature for listed RFCs is not claimed.

MIBs

MIB	MIB 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 IP SLAs VoIP UDP Jitter Operations

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 18: Feature Information for the IP SLAs VoIP UDP Jitter Operation

Feature Name	Releases	Feature Information
IP SLAs - UDP Based VoIP Operation		The 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.
IP SLAs for IPv6 (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)		Support was added for operability in IPv6 networks.

Glossary

codec --In the context of IP Telephony, a codec is a compression and decompression algorithm used to transfer voice and video data more efficiently. Voice codec types are typically referred to using the ITU recommendation number that defines the algorithm (for example, “G.711” instead of “PCM”).

CS-ACELP --The codec type defined in the reference documents G.729 and G.729A, *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)* .

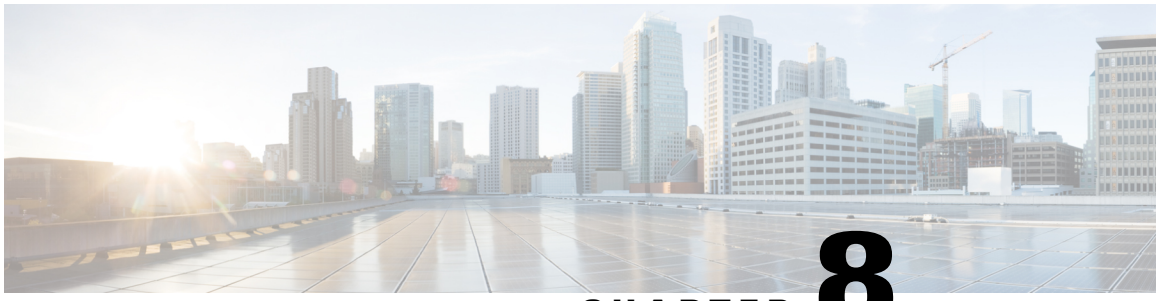
ITU --The International Telecommunication Union. The ITU is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T), responsible for defining standards (Recommendations) covering all fields of telecommunications, is one of the three operational sectors of the ITU. The ITU web site is at http://www.itu.int.

ITU-T --ITU Telecommunication Standardization Sector. The ITU-T is one of the three operational sectors of the ITU, and is responsible for defining standards (called ITU-T Recommendations) covering all fields of telecommunications.

MOS-CQE (Mean Opinion Score; Conversational Quality, Estimated)--The score calculated by a network planning model which aims at predicting the quality in a conversational application situation. Estimates of conversational quality carried out according to ITU-T Rec. G.107, when transformed to a mean opinion score (MOS), give results in terms of MOS-CQE.[3]

PCM --The codec type defined in the reference document G.711, *Pulse code modulation (PCM) of voice frequencies* .

[3] Definition from ITU-T Recommendation P.800.1. Used in accordance with the ITU Copyright and Disclaimer Notice.



CHAPTER 8

IP SLAs Multicast Support

This module describes how to configure and schedule an IP Service Level Agreements (SLAs) multicast UDP jitter operation for measuring and reporting statistics such as one way latency, jitter, and packet loss for each multicast receiver in a user-specified multicast group. .

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.

Prerequisites for IP SLAs Multicast Support

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

between the source and target devices, one-way jitter and packet loss data will be returned, but values of "0" will be returned for the one-way delay measurements provided by the UDP jitter operation.

- All devices must be part of the same VRF in order for IP SLAs multicast operations to succeed.
- The devices on which the responder and probe are to configured must both be running Cisco software images that support the IP SLAs Multicast Support feature. Before configuring any IP SLAs application, use the **show ip sla application** command to verify that the operation type is supported on your software image.

Restrictions for IP SLAs Multicast Support

The multicast UDP Jitter operation can provide only One Way (OW) data.

Information About IP SLAs Multicast Support

Multicast UDP Jitter Operations

A multicast UDP jitter operation measures and reports statistics, such as one way latency, jitter, and packet loss, for each multicast receiver in a user-specified multicast group. Multicast UDP jitter operations enable you to perform the following tasks:

- Analyze and evaluate the performance of a multicast network after deploying a new multicast network application or implementing new multicast-based protocols on the network.
- Check the network behavior for multicast before actually utilizing the multicast network for an important event.
- Take a proactive approach to monitoring a network to isolate possible problem areas.

The sender in a multicast UDP jitter operation sends UDP packets at a specified interval from the source device to a multicast IP address. During the initial configuration, a specified endpoint list provides a list of all the responders to be contacted for a given multicast operation. The multicast subsystem sends a unicast control packet to each of the multicast receivers in the endpoint list, utilizing the unicast path. A control message is sent to each receiver so that it can join the multicast group.

The IP SLAs multicast responder on the multicast receiver receives the UDP packets and records the time-stamp data.

A list of valid responders that have completed a successful IGMP join is maintained on the sender side. Once the responder list is received, multicast packet generation can proceed.

Because all multicast traffic is one way, from sender on the source to responder on the receiver, each responder that is part of the operation is responsible for performing local calculations and for storing the statistics. The statistics are sent back to the sender to be displayed at the end of each cycle of the operation (after all packets have been transmitted to the responder). Because the responder does not maintain a history of the statistics, and also releases all associated memory after sending the information to the sender, each scheduled operation (based on the frequency) is considered a new operation by the multicast responder, with no relationship to the previous one.

Multicast UDP jitter operations are supported in IPv4 networks.

How to Configure IP SLAs Multicast Support

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** *ip-address* **port** *port***vrf** *vrf*	(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:
	`Device(config)# ip sla responder`
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		• Protocol control is enabled by default.

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

Creating a List of Multicast Responders on the Source Device

Before You Begin

All responders to be added to the endpoint list (of responders) must first be configured on the destination device. For configuration information, see the "Configuring an IP SLAs Responder on the Destination Device" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla endpoint-list type ip** *template-name*
4. **description** *description*
5. **ip-address** *address* [**-***address* | **,** *...* **,** *address*] **port** *port*
6. **end**
7. **show ip sla endpoint-list** [**type ip** [*template-name*]]

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 endpoint-list type ip** *template-name* **Example:** `Device(config)# ip sla endpoint-list type ip mcast-rcvrs`	Begins configuring an endpoint list and enters endpoint-list configuration mode.
Step 4	**description** *description* **Example:** `Device(config-epl)# description list of receivers`	(Optional) Adds descriptive text to the template being configured.
Step 5	**ip-address** *address* [**-***address* | **,** *... ,* *address*] **port** *port* **Example:** `Device(config-epl)# ip-address 10.1.1.1-13 port 6500`	Adds the IPv4 or IPv6 address of a multicast responder to the endpoint list being configured. • Repeat this command until all desired addresses are configured. • Use the **no** from of this command to modify the endpoint list by removing one or more addresses.
Step 6	**end** **Example:** `Device(config-epl)# end`	Returns to privileged EXEC mode.
Step 7	**show ip sla endpoint-list** [**type ip** [*template-name*]] **Example:** `Device# show ip sla endpoint-list type ip mcast-rcvrs`	(Optional) Displays the configuration of the endpoint list.

Configuring Multicast UDP Jitter Operations

Note

- 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. Therefore, 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 will 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).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **endpoint-list** *endpoint-list* [**ssm**] [**source-ip** *ip-address*] [**source-port** *port-number*] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **control retry** *retries*
6. **control timeout** *seconds*
7. **dscp** *dscp-value*
8. **tree-init** *number*
9. **history distributions-of-statistics-kept** *size*
10. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
11. **frequency** *seconds*
12. **history hours-of-statistics-kept** *hours*
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. **tos** *number*
20. **verify-data**
21. **vrf** *vrf-name*
22. **end**
23. **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`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* **endpoint-list** *endpoint-list* [**ssm**] [**source-ip** *ip-address*] [**source-port** *port-number*] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] **Example:** `Device(config-ip-sla)# udp-jitter 239.1.1.1 5000 endpoint-list mcast-rcvrs source-ip 10.10.10.106 source-port 7012 num-packets 50 interval 25`	Configures the IP SLAs operation as a multicast UDP jitter operation and enters multicast UDP jitter configuration mode.
Step 5	**control retry** *retries* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# control retry 2`	(Optional) Configures the number of times a sending device will resend a control protocol message.
Step 6	**control timeout** *seconds* **Example:** `Device(config-ip-sla-multicast-jitter)# control timeout 4`	(Optional) Configures the number of seconds that the destination device will wait for a control protocol message.
Step 7	**dscp** *dscp-value* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# dscp 10`	(Optional) Configures the DSCP value for the operation.

	Command or Action	Purpose
Step 8	**tree-init** *number* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# tree-init 1`	(Optional) Sets up the multicast tree.
Step 9	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 10	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Device(config-ip-sla-multicast-jitter-oper)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 11	**frequency** *seconds* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 12	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 13	**owner** *owner-id* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	**request-data-size** *bytes* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.

	Command or Action	Purpose
Step 15	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	**tag** *text* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	**tos** *number* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# tos 160`	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 20	**verify-data** **Example:** `Device(config-ip-sla-multicast-jitter-oper)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 21	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-multicast-jitter-oper)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) VPNs using IP SLAs operations.
Step 22	**end** **Example:** `Device(config-ip-sla-multicast-jitter-oper)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 23	**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.

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** *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*]}]
	
	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 Multicast Support

Example: Multicast UDP Jitter Operation

```
Device# show ip sla endpoint-list

Endpoint-list Name: multicast
    Description:
    ip-address 192.0.2.1 port 1111
    ip-address 192.0.2.2 port 2222
    ip-address 192.0.2.3 port 3333
Device# show ip sla configuration 22

IP SLAs Infrastructure Engine-III
Entry number: 22
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 224.1.1.1/0.0.0.0
Target port/Source port: 2460/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 32
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
```

```
Enhanced History:

  sno     oper-id              dest-ip-addr  !<---Responders in endpoint list: multicast
    1    976271337             192.0.2.1
    2   1632881300             192.0.2.2
    3   2138021658             192.0.2.3
```

Additional References for IP SLAs Multicast Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP SLAs commands	Cisco IOS IP SLAs Command Reference
Information about Cisco IP SLAs	"Cisco IOS IP SLAs Overview" module of the *IP SLAs Configuration Guide*

MIBs

MIB	MIBs Link
CISCO-IPSLA-TC-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

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

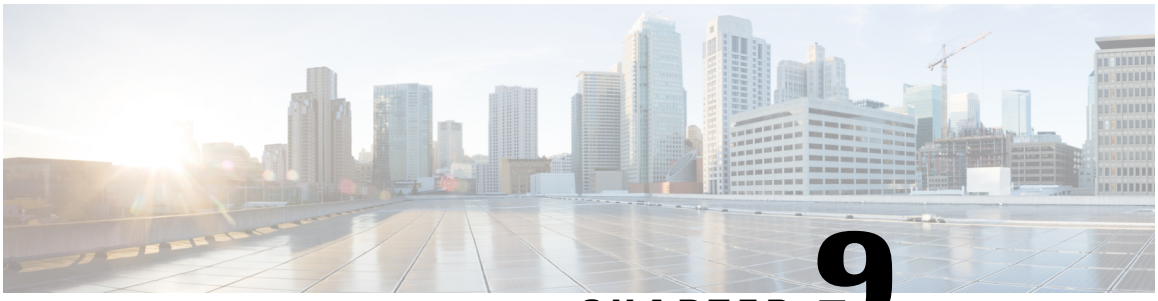
Feature Information for IPSLA Multicast Support

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 19: Feature Information for IPSLA Multicast Support

Feature Name	Releases	Feature Information
IPSLA Multicast Support	15.2(4)M 15.3(1)S Cisco IOS XE Release 3.8S 15.1(2)SG Cisco IOS XE Release 3.4SG	This feature introduced the multicast UDP jitter operation for measuring and reporting statistics such as one way latency, jitter, and packet loss for each multicast receiver in a user-specified multicast group. The following commands were introduced or modified: **clock-tolerance ntp oneway**, **control (IP SLA)**, **dscp (IP SLA)**, **history distributions-of-statistics-kept**, **history enhanced**, **history hours-of-statistics-kept**, **ip-address (endpoint list)**, **operation-packet priority**, **owner**, **precision**, **show ip sla application**, **show ip sla configuration**, **show ip sla endpoint-list**, **show ip sla statistics**, **show ip sla statistics aggregated**, **tag (IP SLA)**, **timeout (IP SLA)**, **tos**, **tree-init**, **udp-jitter**, **verify-data (IP SLA)**, **vrf**.



CHAPTER 9

Configuring IP SLAs LSP Health Monitor Operations

This module describes how to configure an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor. LSP health monitors enable you to to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides automated end-to-end verification in the control plane and data plane for all LSPs between the participating Provider Edge (PE) devices. This end-to-end (PE-to-PE device) approach ensures that LSP connectivity is verified along the paths that customer traffic is sent. Consequently, customer-impacting network connectivity issues that occur within the MPLS core will be detected by the LSP Health Monitor. Once configured, the LSP Health Monitor will automatically create and delete IP SLAs LSP ping or LSP traceroute operations based on network topology.

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.

Prerequisites for LSP Health Monitor Operations

- The participating PE devices of an LSP Health Monitor operation must support the MPLS LSP ping feature. It is recommended that the Provider (P) devices also support the MPLS LSP Ping feature in order to obtain complete error reporting and diagnostics information.
- Ensure that the source PE device has enough memory to support the desired LSP Health Monitor functionality. Enabling the LSP discovery option can potentially have a significant impact on device memory. If there is not enough memory available during the LSP discovery process, the process will gracefully terminate and an error message will be displayed.

Note The destination PE devices of an LSP Health Monitor operation do not require the IP SLAs Responder to be enabled.

Restrictions for LSP Health Monitor Operations

- Once an LSP Health Monitor operation is started, its configuration parameters should not be changed until the operation has ended. Changing the configuration parameters while the operation is actively running could cause delays in obtaining network connectivity statistics.

Information About LSP Health Monitor Operations

Benefits of the LSP Health Monitor

- End-to-end LSP connectivity measurements across equal-cost multipaths for determining network availability or testing network connectivity in MPLS networks
- Proactive threshold monitoring through SNMP trap notifications and syslog messages
- Reduced network troubleshooting time for MPLS networks
- Scalable network error detection using fast retry capability
- Creation and deletion of IP SLAs operations based on network topology
- Discovery of Border Gateway Protocol (BGP) next hop neighbors based on local VPN routing and forwarding instances (VRFs) and global routing tables
- Multioperation scheduling of IP SLAs operations
- Pseudo-wire connectivity testing between MPLS network edges, with threshold violations and scalable operation scheduling
- Monitoring and SNMP trap alerts for round-trip time (RTT) threshold violations, connection loss, and command response timeouts

How the LSP Health Monitor Works

The LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs. The general process for how the LSP Health Monitor works is as follows:

1. The user configures an LSP Health Monitor operation and the BGP next hop neighbor discovery process is enabled.
   Configuring an LSP Health Monitor operation is similar to configuring a standard IP SLAs operation. To illustrate, all operation parameters for an LSP Health Monitor operation are configured after an identification number for the operation is specified. However, unlike standard IP SLAs operations, these configured parameters are then used as the base configuration for the individual IP SLAs LSP ping and LSP traceroute operations that will be created by the LSP Health Monitor. The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE device. To prevent unnecessary device performance issues, careful consideration should be taken when configuring the operational and scheduling parameters of an LSP Health Monitor operation.

   When the BGP next hop neighbor discovery process is enabled, a database of BGP next hop neighbors in use by any VRF associated with the source PE device is generated based on information from the local VRF and global routing tables. For more information about the BGP next hop neighbor discovery process, see the "Discovery of Neighboring PE Devices" section.

Note By default, only a single path between the source and destination PE devices is discovered. If the LSP discovery option is enabled, the equal-cost multipaths between the source and destination PE devices are discovered. For more information on how the LSP discovery process works, see the "LSP Discovery Process" section.

2. The user configures proactive threshold monitoring parameters for the LSP Health Monitor operation. For more information about proactive threshold monitoring, see the "Proactive Threshold Monitoring for the LSP Health Monitor" section.
   Depending on the proactive threshold monitoring configuration options chosen, SNMP trap notifications or syslog messages are generated as threshold violations are met.
3. The user configures multioperation scheduling parameters for the LSP Health Monitor operation. For more information about multioperation scheduling, see the "Multioperation Scheduling for the LSP Health Monitor" section.
   Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created (based on parameters configured in Step 1) for each applicable PE (BGP next hop) neighbor. The IP SLAs operations will measure network connectivity between the source PE device and the discovered destination PE device. The start time and frequency of each measurement is based on the multioperation scheduling parameters defined by the user.

Addition and Deletion of IP SLAs Operations

The LSP Health Monitor receives periodic notifications about BGP next hop neighbors that have been added to or removed from a particular VPN. This information is stored in a queue maintained by the LSP Health Monitor. Based on the information in the queue and user-specified time intervals, new IP SLAs operations are automatically created for newly discovered PE devices and existing IP SLAs operations are automatically deleted for any PE devices that are no longer valid. The automatic deletion of operations can be disabled. However, disabling this function is not recommended because these operations would then need to be deleted manually.

If the LSP discovery option is enabled, creation of LSP discovery groups for newly discovered BGP next hop neighbors will follow the same process as described in the "LSP Discovery Process" section. If a BGP next hop neighbor is removed from a particular VPN, all the corresponding LSP discovery groups and their associated individual IP SLAs operations and statistics are removed from the LSP discovery group database.

Access Lists for Filtering BGP Next Hop Neighbors

Standard IP access lists can be configured to restrict the number of IP SLAs operations that are automatically created by the LSP Health Monitor. When the IP SLAs access list parameter is configured, the list of BGP next hop neighbors discovered by the LSP Health Monitor is filtered based on the conditions defined by the associated standard IP access list. In other words, the LSP Health Monitor will automatically create IP SLAs operations only for those BGP next hop neighbors with source addresses that satisfy the criteria permitted by the standard IP access list.

Unique Identifier for Each Automatically Created IP SLAs Operation

The IP SLAs operations automatically created by the LSP Health Monitor are uniquely identified by their owner field. The owner field of an operation is generated using all the parameters that can be configured for that particular operation. If the length of the owner field is longer than 255 characters, it will be truncated.

Discovery of Neighboring PE Devices

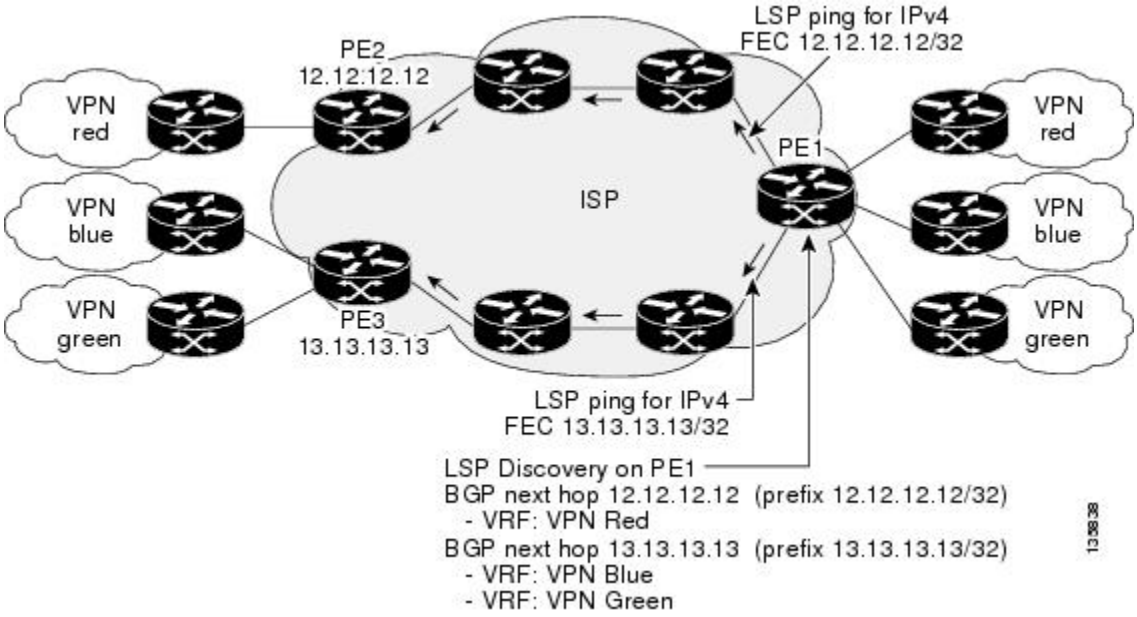
A BGP next hop neighbor discovery process is used to find the BGP next hop neighbors in use by any VRF associated with the source PE device. In most cases, these neighbors will be PE devices.

When the BGP next hop neighbor discovery process is enabled, a database of BGP next hop neighbors in use by any VRF associated with the source PE device is generated based on information from the local VRF and global routing tables. As routing updates are received, new BGP next hop neighbors are added to and deleted from the database immediately.

The figure below shows how the BGP next hop neighbor discovery process works for a simple VPN scenario for an Internet service provider (ISP). In this example, there are three VPNs associated with device PE1: red, blue, and green. From the perspective of device PE1, these VPNs are reachable remotely through BGP next hop neighbors PE2 (device ID: 12.12.12.12) and PE3 (device ID: 13.13.13.13). When the BGP next hop neighbor discovery process is enabled on device PE1, a database is generated based on the local VRF and global routing tables. The database in this example contains two BGP next hop device entries: PE2 12.12.12.12 and PE3 13.13.13.13. The routing entries are maintained per next hop device to distinguish which next hop devices belong within which particular VRF. For each next hop device entry, the IPv4 Forward Equivalence

Class (FEC) of the BGP next hop device in the global routing table is provided so that it can be used by the MPLS LSP ping operation.

Figure 4: BGP Next Hop Neighbor Discovery for a Simple VPN



LSP Discovery

The LSP discovery option of an LSP Health Monitor operation provides the capability to discover the equal-cost multipaths for carrying MPLS traffic between the source and destination PE devices. Network connectivity measurements can then be performed for each of the paths that were discovered.

The general process for LSP discovery is as follows:

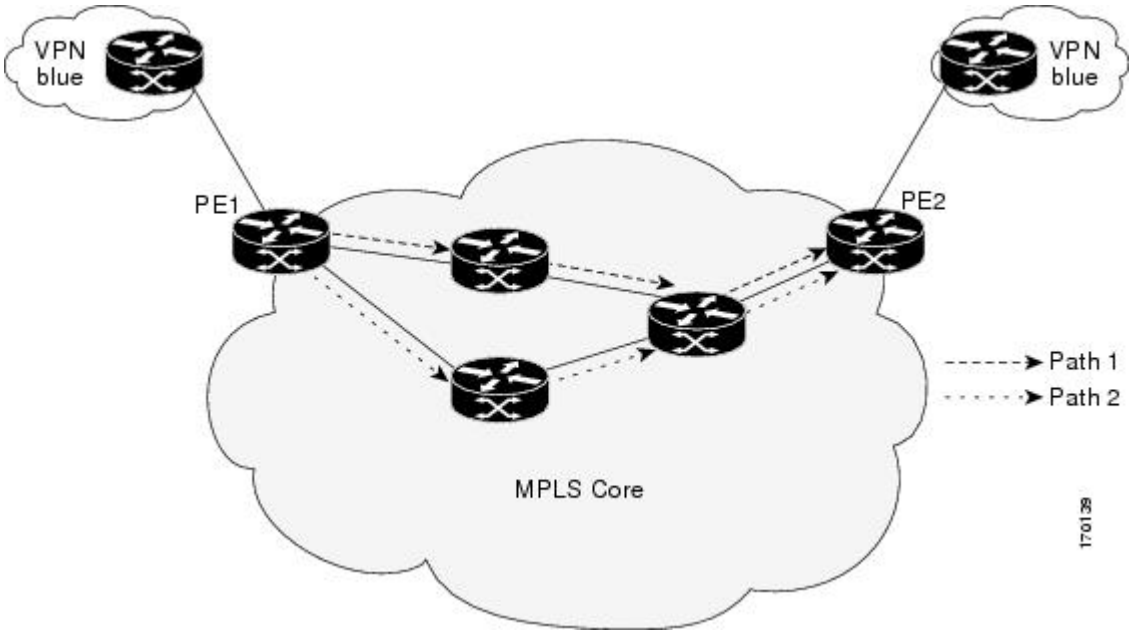
1. BGP next hop neighbors are discovered using the BGP next hop neighbor discovery process. For more information about the BGP next hop neighbor discovery process, see the "Discovery of Neighboring PE Routers" section.
   Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created for each applicable PE (BGP next hop) neighbor. Only a single path to each applicable PE neighbor is discovered during this initial step of the LSP discovery process. For each next hop neighbor, the LSP Health Monitor creates an LSP discovery group (that initially consists of only the one discovered path) and assigns the group with a unique identification number. For more information about LSP discovery groups, see the "LSP Discovery Groups" section.
2. An LSP discovery request is sent by the LSP Health Monitor to the LSP discovery subsystem for each applicable BGP next hop neighbor. For each next hop neighbor in which an appropriate response is received, MPLS echo requests are sent one-by-one from the source PE device to discover the equal-cost multipaths. The parameters that uniquely identify each equal-cost multipath (127/8 destination IP address [LSP selector] and the PE outgoing interface) are added to the associated LSP discovery database.

Note For a given LSP Health Monitor operation, the user can define the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery.

3. Each individual IP SLAs operation (created for each applicable PE neighbor) uses an IP SLAs LSP ping superoperation to measure network connectivity across all equal-cost multipaths between the source PE device and discovered destination PE device. The IP SLAs superoperation operates by sending an LSP ping packet to the destination PE device and adjusting the LSP ping 127/8 LSP selector IP address for each discovered equal-cost multipath. For example, assume that there are three equal-cost multipaths to a destination PE device and the identified LSP selector IP addresses are 127.0.0.1, 127.0.0.5, and 127.0.0.6. The IP SLAs superoperation would sequentially send three LSP ping packets using the identified LSP selector IP addresses for directing the superoperation across the three paths. This technique ensures that there is only a single IP SLAs LSP ping operation for each source and destination PE device pair, and significantly reduces the number of active LSP ping operations sent by the source PE device.

The figure below illustrates a simple VPN scenario. This network consists of a core MPLS VPN with two PE devices (device PE1 and device PE2) belonging to the VRF named VPN blue. Suppose device PE1 is the source PE device for an LSP Health Monitor operation with the LSP discovery option enabled and that device PE2 is discovered by the BGP discovery process as a BGP next hop neighbor to device PE1. If path 1 and path 2 are equal-cost multipaths between device PE1 to device PE2, then the LSP discovery process would create an LSP discovery group consisting of path 1 and path 2. An IP SLAs LSP ping superoperation would also be created to monitor network availability across each path.

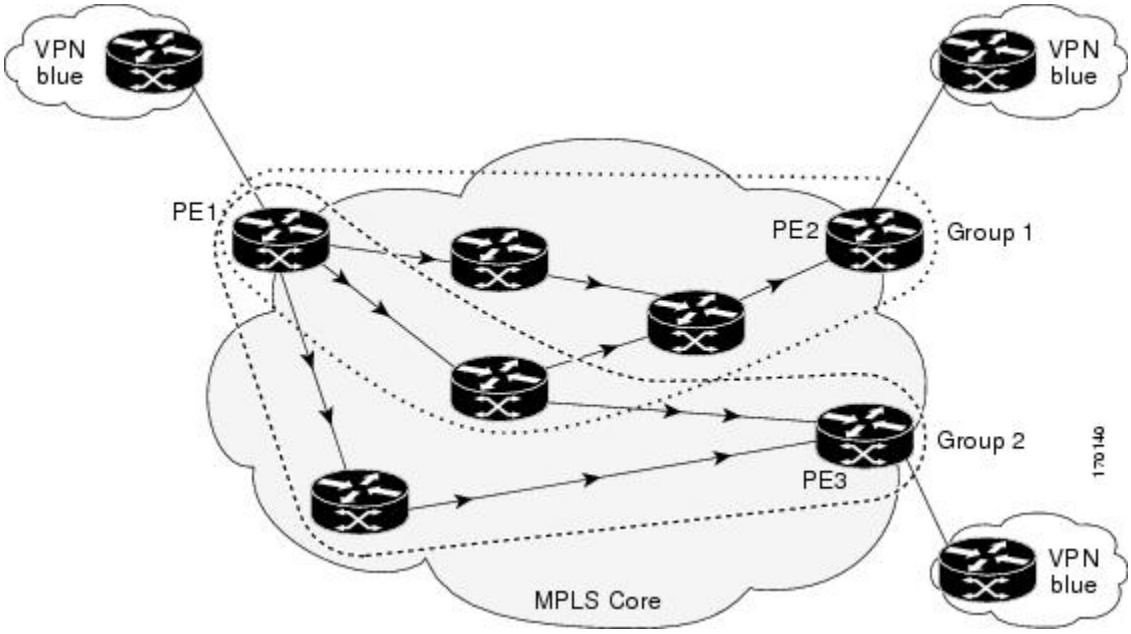
Figure 5: LSP Discovery for a Simple VPN



LSP Discovery Groups

A single LSP Health Monitor operation can be comprised of several LSP discovery groups depending on the number of BGP next hop neighbors discovered by the BGP next hop neighbor discovery process. Each LSP discovery group corresponds to one BGP next hop neighbor and is assigned a unique identification number (starting with the number 1). The figure below illustrates a simple VPN scenario. This network consists of a core MPLS VPN with three PE devices (device PE1, PE2, and PE3) belonging to the VRF named VPN blue. Suppose device PE1 is the source PE device for an LSP Health Monitor operation with the LSP discovery option enabled and that device PE2 and PE3 are discovered by the BGP discovery process as BGP next hop neighbors to device PE1. LSP discovery group 1 is created for the equal-cost multipaths between device PE1 to device PE2 and LSP discovery group 2 is created for the equal-cost multipaths between device PE1 to device PE3.

Figure 6: LSP Discovery Groups for a Simple VPN



Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created for each applicable PE (BGP next hop) neighbor. Each IP SLAs operation (created for each applicable PE neighbor) uses an IP SLAs LSP ping superoperation to measure network connectivity across all equal-cost multipaths between the source PE device and discovered destination PE device. Each LSP ping superoperation corresponds to a single LSP discovery group.

The LSP ping superoperation operates by sending an LSP ping packet to the destination PE device and adjusting the LSP ping 127/8 LSP selector IP address for each discovered equal-cost multipath. The network connectivity statistics collected by each equal-cost multipath is aggregated and stored in one-hour increments (data can be collected for a maximum of two hours). Results are stored as group averages representative of all the equal-cost multipaths within the LSP discovery group for a given one-hour increment.

Each equal-cost multipath discovered between the source PE device and a BGP next hop neighbor is uniquely identified with the following parameters:

- 127/8 destination IP address (LSP selector) within the local host IP address range

- PE outgoing interface

The database for an LSP discovery group is updated if any of the following events occur:

- The corresponding LSP ping superoperation sends an LSP ping packet.
- An active equal-cost multipath is added to or deleted from the LSP discovery group.
- The user enters the Cisco command to delete all the aggregated statistical data for a particular LSP discovery group.

IP SLAs LSP Ping and LSP Traceroute

The LSP Health Monitor feature introduces support for the IP SLAs LSP ping and IP SLAs LSP traceroute operations. These operations are useful for troubleshooting network connectivity issues and determining network availability in an MPLS VPN. When using the LSP Health Monitor, IP SLAs LSP ping and LSP traceroute operations are automatically created to measure network connectivity between the source PE device and the discovered destination PE devices. Individual IP SLAs LSP ping and LSP traceroute operations can also be manually configured. Manual configuration of these operations can be useful for troubleshooting a connectivity issue.

The IP SLAs LSP ping and IP SLAs LSP traceroute operations are based on the same infrastructure used by the MPLS LSP Ping and MPLS LSP Traceroute features, respectively, for sending and receiving echo reply and request packets to test LSPs.

The LSP discovery does not support IP SLAs traceroute operations.

Proactive Threshold Monitoring for the LSP Health Monitor

Proactive threshold monitoring support for the LSP Health Monitor feature provides the capability for triggering SNMP trap notifications and syslog messages when user-defined reaction conditions (such as a connection loss or timeout) are met. Configuring threshold monitoring for an LSP Health Monitor operation is similar to configuring threshold monitoring for a standard IP SLAs operation.

LSP Discovery Option Enabled

If the LSP discovery option for an LSP Health Monitor operation is enabled, SNMP trap notifications can be generated when one of the following events occurs:

- LSP discovery for a particular BGP next hop neighbor fails.
- Operational status of an LSP discovery group changes.

Possible reasons for which LSP discovery can fail for a particular BGP next hop neighbor are as follows:

- Expiration of time allowed for a BGP next hop neighbor to respond to an LSP discovery request.
- Return code is “Broken” or “Unexplorable” for all paths leading to the BGP next hop neighbor.

The table below describes the conditions for which the operational status of an LSP discovery group can change. Whenever an individual IP SLAs LSP ping operation of an LSP discovery group is executed, a return code is generated. Depending on the value of the return code and the current status of the LSP discovery group, the group status can change.

Table 20: Conditions for Which an LSP Discovery Group Status Changes

Individual IP SLAs Operation Return Code	Current Group Status = UP	Current Group Status = PARTIAL	Current Group Status = DOWN
OK	No group status change.	If return codes for all paths in the group are OK, then the group status changes to UP.	Group status changes to PARTIAL.
Broken or Unexplorable	Group status changes to PARTIAL.	If return codes for all paths in the group are Broken or Unexplorable, then the group status changes to DOWN.	No group status change.

The return code for an individual IP SLAs LSP ping operation can be one of the following:

- OK--Indicates that the LSP is working properly. The customer VPN traffic will be sent across this path.
- Broken--Indicates that the LSP is broken. Customer VPN traffic will not be sent across this path and may be discarded.
- Unexplorable--Indicates that not all the paths to this PE neighbor have been discovered. This may be due to a disruption along the LSP or because the number of 127/8 IP addresses used for LSP selection has been exhausted.

The status of an LSP discovery group can be one of the following:

- UNKNOWN--Indicates that group status has not yet been determined and that the paths belonging to the group are in the process of being tested for the first time. Once this initial test is complete, the group status will change to UP, PARTIAL, or DOWN.
- UP--Indicates that all the paths within the group are active and no operation failures have been detected.
- PARTIAL--Indicates that an operation failure has been detected for one or more, but not all, of the paths within the group.
- DOWN--Indicates that an operation failure has been detected for all the paths within the group.

Secondary Frequency Option

With the introduction of the LSP Health Monitor feature, a new threshold monitoring parameter has been added that allows you to specify a secondary frequency. If the secondary frequency option is configured and a failure (such as a connection loss or timeout) is detected for a particular path, the frequency at which the path is remeasured will increase to the secondary frequency value (testing at a faster rate). When the configured reaction condition is met (such as N consecutive connection losses or N consecutive timeouts), an SNMP trap and syslog message can be sent and the measurement frequency will return to its original frequency value.

Multioperation Scheduling for an LSP Health Monitor

Multioperation scheduling support for the LSP Health Monitor feature provides the capability to easily schedule the automatically created IP SLAs operations (for a given LSP Health Monitor operation) to begin at intervals equally distributed over a specified duration of time (schedule period) and to restart at a specified frequency. Multioperation scheduling is particularly useful in cases where the LSP Health Monitor is enabled on a source PE device that has a large number of PE neighbors and, therefore, a large number of IP SLAs operations running at the same time.

Newly created IP SLAs operations (for newly discovered BGP next hop neighbors) are added to the same schedule period as the operations that are currently running. To prevent too many operations from starting at the same time, the multioperation scheduling feature will schedule the operations to begin at random intervals uniformly distributed over the schedule period.

Configuring a multioperation schedule for an LSP Health Monitor is similar to configuring a standard multioperation schedule for a group of individual IP SLAs operations.

LSP Discovery Enabled

When a multioperation schedule for an LSP Health Monitor operation with LSP discovery is started, the BGP next hop neighbors are discovered, and network connectivity to each applicable neighbor is monitored using only a single LSP. Initially, network connectivity between the source PE device and discovered destination PE device is measured across only a single path. This initial condition is the same as if an LSP Health Monitor operation was performed without LSP discovery.

Specific information about the IP SLAs LSP ping operations that are created for newly discovered equal-cost paths during the succeeding iterations of the LSP discovery process are stored in the LSP discovery group database. These newly created IP SLAs LSP ping operations will start collecting data at the next iteration of network connectivity measurements for their associated LSP discovery group.

The start times for the individual IP SLAs LSP ping operations for each LSP discovery group is based on the number of LSP discovery groups and the schedule period of the multioperation schedule. For example, if three LSP discovery groups (Group 1, Group 2, and Group 3) are scheduled to run over a period of 60 seconds, the first LSP ping operation of Group 1 will start at 0 seconds, the first LSP ping operation of Group 2 will start at 20 seconds, and the first LSP ping operation of Group 3 will start at 40 seconds. The remaining individual IP SLAs LSP ping operations for each LSP discovery group will run sequentially after completion of the first LSP ping operation. For each LSP discovery group, only one LSP ping operation runs at a time.

How to Configure LSP Health Monitor Operations

Configuring an LSP Health Monitor Operation

Perform only one of the following tasks:

Configuring an LSP Health Monitor Operation without LSP Discovery on a PE Device

Note If LSP discovery is disabled, only a single path between the source PE device and each BGP next hop neighbor is discovered.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval** *seconds*
5. **auto ip sla mpls-lsp-monitor** *operation-number*
6. Do one of the following:
   - **type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
   - **type pathEcho** [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. **access-list** *access-list-number*
8. **scan-interval** *minutes*
9. **delete-scan-factor** *factor*
10. **force-explicit-null**
11. **exp** *exp-bits*
12. **lsp-selector** *ip-address*
13. **reply-dscp-bits** *dscp-value*
14. **reply-mode** {**ipv4** | **router-alert**}
15. **request-data-size** *bytes*
16. **secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency*
17. **tag** *text*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **ttl** *time-to-live*
21. **exit**
22. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}]
23. **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	**mpls discovery vpn next-hop** **Example:** `Device(config)# mpls discovery vpn next-hop`	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process. **Note** This command is automatically enabled when the **auto ip sla mpls-lsp-monitor** command is entered.
Step 4	**mpls discovery vpn interval** *seconds* **Example:** `Device(config)# mpls discovery vpn interval 120`	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
Step 5	**auto ip sla mpls-lsp-monitor** *operation-number* **Example:** `Device(config)# auto ip sla mpls-lsp-monitor 1`	Begins configuration for an LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode. **Note** Entering this command automatically enables the **mpls discovery vpn next-hop** command.

Step 6	Do one of the following:
	• **type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
	• **type pathEcho** [**ipsla-vrf-all** | **vrf** *vpn-name*]
	Example:
	`Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`
	Example:
	`Device(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all`
		Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.
		or
		Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP traceroute operation using the LSP Health Monitor.

Step 7	**access-list** *access-list-number* **Example:** `Device(config-auto-ip-sla-mpls-params)# access-list 10`	(Optional) Specifies the access list to apply to an LSP Health Monitor operation.

	Command or Action	Purpose
Step 8	**scan-interval** *minutes* **Example:** `Device(config-auto-ip-sla-mpls-params)# scan-interval 5`	(Optional) Sets the timer for the IP SLAs LSP Health Monitor database.
Step 9	**delete-scan-factor** *factor* **Example:** `Device(config-auto-ip-sla-mpls-params)# delete-scan-factor 2`	(Optional) Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid. • The default scan factor is 1. Each time the LSP Health Monitor checks the scan queue for updates, it deletes IP SLAs operations for BGP next hop neighbors that are no longer valid. • If the scan factor is set to 0, IP SLAs operations will not be automatically deleted by the LSP Health Monitor. This configuration is not recommended. • This command must be used with the **scan-interval** command.
Step 10	**force-explicit-null** **Example:** `Device(config-auto-ip-sla-mpls-params)# force-explicit-null`	(Optional) Adds an explicit null label to all echo request packets of an IP SLAs operation.
Step 11	**exp** *exp-bits* **Example:** `Device(config-auto-ip-sla-mpls-params)# exp 5`	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.
Step 12	**lsp-selector** *ip-address* **Example:** `Device(config-auto-ip-sla-mpls-params)# lsp-selector 127.0.0.10`	(Optional) Specifies the local host IP address used to select the LSP of an IP SLAs operation.
Step 13	**reply-dscp-bits** *dscp-value* **Example:** `Device(config-auto-ip-sla-mpls-params)# reply-dscp-bits 5`	(Optional) Specifies the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation.

	Command or Action	Purpose
Step 14	**reply-mode** {**ipv4** | **router-alert**} **Example:** `Device(config-auto-ip-sla-mpls-params)# reply-mode router-alert`	(Optional) Specifies the reply mode for an echo request packet of an IP SLAs operation. • The default reply mode is an IPv4 UDP packet.
Step 15	**request-data-size** *bytes* **Example:** `Device(config-auto-ip-sla-mpls-params)# request-data-size 200`	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
Step 16	**secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency* **Example:** `Device(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10`	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.
Step 17	**tag** *text* **Example:** `Device(config-auto-ip-sla-mpls-params)# tag testgroup`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	**threshold** *milliseconds* **Example:** `Device(config-auto-ip-sla-mpls-params)# threshold 6000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 19	**timeout** *milliseconds* **Example:** `Device(config-auto-ip-sla-mpls-params)# timeout 7000`	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
Step 20	**ttl** *time-to-live* **Example:** `Device(config-auto-ip-sla-mpls-params)# ttl 200`	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.

	Command or Action	Purpose
Step 21	**exit** **Example:** `Device(config-auto-ip-sla-mpls-params)# exit`	Exits MPLS parameters configuration submode and returns to global configuration mode.
Step 22	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}] **Example:** `Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss action-type trapOnly threshold-type consecutive 3`	(Optional) Configures certain actions to occur based on events under the control of the LSP Health Monitor.
Step 23	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Device

Note

- The LSP Health Monitor with LSP Discovery feature supports Layer 3 MPLS VPNs only.
- The LSP discovery option does not support IP SLAs LSP traceroute operations.
- The LSP discovery option does not support IP SLAs VCCV operations.
- The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE device. To prevent unnecessary device performance issues, careful consideration should be taken when configuring the operational and scheduling parameters of an LSP Health Monitor operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval** *seconds*
5. **auto ip sla mpls-lsp-monitor** *operation-number*
6. **type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. Configure optional parameters for the IP SLAs LSP echo operation.
8. **path-discover**
9. **hours-of-statistics-kept** *hours*
10. **force-explicit-null**
11. **interval** *milliseconds*
12. **lsp-selector-base** *ip-address*
13. **maximum-sessions** *number*
14. **scan-period** *minutes*
15. **session-timeout** *seconds*
16. **timeout** *seconds*
17. **exit**
18. **exit**
19. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**]
20. **ip sla logging traps**
21. **exit**

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	**mpls discovery vpn next-hop** **Example:** `Device(config)# mpls discovery vpn next-hop`	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process. **Note** This command is automatically enabled when the **auto ip sla mpls-lsp-monitor** command is entered.

	Command or Action	Purpose
Step 4	**mpls discovery vpn interval** *seconds* **Example:** `Device(config)# mpls discovery vpn interval 120`	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
Step 5	**auto ip sla mpls-lsp-monitor** *operation-number* **Example:** `Device(config)# auto ip sla mpls-lsp-monitor 1`	Begins configuration for an LSP Health Monitor operation and enters auto IP SLAs MPLS configuration mode. **Note** Entering this command automatically enables the **mpls discovery vpn next-hop** command.
Step 6	**type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*] **Example:** `Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`	Enters MPLS parameters configuration mode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.
Step 7	Configure optional parameters for the IP SLAs LSP echo operation.	(Optional) See Steps 7 through 21 in the "Configuring an LSP Health Monitor Operation Without LSP Discovery on a PE Device" section.
Step 8	**path-discover** **Example:** `Device(config-auto-ip-sla-mpls-params)# path-discover`	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters LSP discovery parameters configuration submode.
Step 9	**hours-of-statistics-kept** *hours* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# hours-of-statistics-kept 1`	(Optional) Sets the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.
Step 10	**force-explicit-null** **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# force-explicit-null`	(Optional) Adds an explicit null label to all echo request packets of an LSP Health Monitor operation.
Step 11	**interval** *milliseconds* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# interval 2`	(Optional) Specifies the time interval between MPLS echo requests that are sent as part of the LSP discovery process for an LSP Health Monitor operation.

	Command or Action	Purpose
Step 12	**lsp-selector-base** *ip-address* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# lsp-selector-base 127.0.0.2`	(Optional) Specifies the base IP address used to select the LSPs belonging to the LSP discovery groups of an LSP Health Monitor operation.
Step 13	**maximum-sessions** *number* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# maximum-sessions 2`	(Optional) Specifies the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation. **Note** Careful consideration should be used when configuring this parameter to avoid a negative impact on the device's CPU.
Step 14	**scan-period** *minutes* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# scan-period 30`	(Optional) Sets the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.
Step 15	**session-timeout** *seconds* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# session-timeout 60`	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its LSP discovery request for a particular BGP next hop neighbor.
Step 16	**timeout** *seconds* **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# timeout 4`	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its echo request packets. **Note** Careful consideration should be used when configuring this parameter to avoid a negative impact on the device's CPU.
Step 17	**exit** **Example:** `Device(config-auto-ip-sla-mpls-lpd-params)# exit`	Exits LSP discovery parameters configuration submode and returns to MPLS parameters configuration mode.
Step 18	**exit** **Example:** `Device(config-auto-ip-sla-mpls-params)# exit`	Exits MPLS parameters configuration mode and returns to global configuration mode.
Step 19	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**]	(Optional) Configures the proactive threshold monitoring parameters for an LSP Health Monitor operation with LSP discovery enabled.

	Command or Action	Purpose
	Example: `Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type trapOnly`	
Step 20	**ip sla logging traps** **Example:** `Device(config)# ip sla logging traps`	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
Step 21	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Scheduling LSP Health Monitor Operations

Note

- The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE device. Careful consideration should be taken when configuring the scheduling parameters to prevent too many IP SLAs LSP ping operations from running at the same time. The schedule period should be set to a relatively large value for large MPLS VPNs.
- Newly created IP SLAs operations (for newly discovered BGP next hop neighbors) are added to the same mulioperation schedule period as the operations that are currently running. To prevent too many operations from starting at the same time, the multioperation scheduler will schedule the operations to begin at random intervals uniformly distributed over the schedule period.

Before You Begin

- All IP SLAs operations to be scheduled must be already configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss* | *hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **now** | **pending**}]
4. **exit**
5. **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	**auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss*	*hh* **:** *mm*[**:** *ss*] [*month day*	*day month*]	**now**	**pending**}] **Example:** `Device(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now`	Configures the scheduling parameters for an LSP Health Monitor operation.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits to privileged EXEC mode.
Step 5	**show ip sla configuration** **Example:** `Device# show ip sla configuration`	(Optional) Displays the IP SLAs configuration details.

Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs LSP ping or LSP traceroute operation. Use the **debug ip sla mpls-lsp-monitor** command to help troubleshoot issues with an IP SLAs LSP Health Monitor operation.

What to Do Next

To display the results of an individual IP SLAs operation use the **show ip sla statistics** and **show ip sla statistics aggregated** commands. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

Manually Configuring and Scheduling an IP SLAs LSP Ping or LSP Traceroute Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. Do one of the following:
   - **mpls lsp ping ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
   - **mpls lsp trace ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
5. **exp** *exp-bits*
6. **request-data-size** *bytes*
7. **secondary-frequency** {**connection-loss** | **timeout**} *frequency*
8. **tag** *text*
9. **threshold** *milliseconds*
10. **timeout** *milliseconds*
11. **ttl** *time-to-live*
12. **exit**
13. **ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]
14. **ip sla logging traps**
15. **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**]
16. **exit**

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 1`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

Step 4	Do one of the following:
	• **mpls lsp ping ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
	• **mpls lsp trace ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
	
	Example:
	`Device(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
	
	Example:
	`Device(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
		• The first example configures the IP SLAs operation as an LSP ping operation and enters LSP ping configuration mode.
		• The second example configures the IP SLAs operation as an LSP trace operation and enters LSP trace configuration mode.

Step 5	**exp** *exp-bits* **Example:** `Device(config-sla-monitor-lspPing)# exp 5`	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation. **Note** The LSP ping configuration mode is used in this example and in the remaining steps. Except where noted, the same commands are also supported in the LSP trace configuration mode.

	Command or Action	Purpose
Step 6	**request-data-size** *bytes* **Example:** `Device(config-sla-monitor-lspPing)# request-data-size 200`	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
Step 7	**secondary-frequency** {**connection-loss** | **timeout**} *frequency* **Example:** `Device(config-sla-monitor-lspPing)# secondary-frequency connection-loss 10`	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs. • This command is for IP SLAs LSP ping operations only. LSP trace configuration mode does not support this command.
Step 8	**tag** *text* **Example:** `Device(config-sla-monitor-lspPing)# tag testgroup`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	**threshold** *milliseconds* **Example:** `Device(config-sla-monitor-lspPing)# threshold 6000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 10	**timeout** *milliseconds* **Example:** `Device(config-sla-monitor-lspPing)# timeout 7000`	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
Step 11	**ttl** *time-to-live* **Example:** `Device(config-sla-monitor-lspPing)# ttl 200`	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.
Step 12	**exit** **Example:** `Device(config-sla-monitor-lspPing)# exit`	Exits LSP ping or LSP trace configuration submode and returns to global configuration mode.
Step 13	**ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]	(Optional) Configures certain actions to occur based on events under the control of IP SLAs.

	Command or Action	Purpose
	Example: `Device(config)# ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type traponly`	
Step 14	**ip sla logging traps** **Example:** `Device(config)# ip sla logging traps`	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
Step 15	**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:** `Device(config)# ip sla schedule 1 start-time now`	Configures the scheduling parameters for an IP SLAs operation.
Step 16	**exit** **Example:** `Device(config)# exit`	Exits global configuration submode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs LSP ping or LSP traceroute operation.

What to Do Next

To display the results of an individual IP SLAs operation use the **show ip sla statistics** and **show ip sla statistics aggregated** commands. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

Verifying and Troubleshooting LSP Health Monitor Operations

SUMMARY STEPS

1. **debug ip sla error** [*operation-number*]
2. **debug ip sla mpls-lsp-monitor** [*operation-number*]
3. **debug ip sla trace** [*operation-number*]
4. **show ip sla mpls-lsp-monitor collection-statistics** [*group-id*]
5. **show ip sla mpls-lsp-monitor configuration** [*operation-number*]
6. **show ip sla mpls-lsp-monitor lpd operational-state** [*group-id*]
7. **show ip sla mpls-lsp-monitor neighbors**
8. **show ip sla mpls-lsp-monitor scan-queue** *operation-number*
9. **show ip sla mpls-lsp-monitor summary** [*operation-number* [**group** [*group-id*]]]
10. **show ip sla statistics** [*operation-number*] [**details**]
11. **show ip sla statistics aggregated** [*operation-number*] [**details**]
12. **show mpls discovery vpn**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**debug ip sla error** [*operation-number*] **Example:** `Device# debug ip sla error`	(Optional) Enables debugging output of IP SLAs operation run-time errors.
Step 2	**debug ip sla mpls-lsp-monitor** [*operation-number*] **Example:** `Device# debug ip sla mpls-lsp-monitor`	(Optional) Enables debugging output of LSP Health Monitor operations.
Step 3	**debug ip sla trace** [*operation-number*] **Example:** `Device# debug ip sla trace`	(Optional) Enables debugging output for tracing the execution of IP SLAs operations.
Step 4	**show ip sla mpls-lsp-monitor collection-statistics** [*group-id*] **Example:** `Device# show ip sla mpls-lsp-monitor collection-statistics 100001`	(Optional) Displays the statistics for IP SLAs operations belonging to an LSP discovery group of an LSP Health Monitor operation. **Note** This command is applicable only if the LSP discovery option is enabled.

	Command or Action	Purpose
Step 5	**show ip sla mpls-lsp-monitor configuration** [*operation-number*] **Example:** `Device# show ip sla mpls-lsp-monitor configuration 1`	(Optional) Displays configuration settings for LSP Health Monitor operations.
Step 6	**show ip sla mpls-lsp-monitor lpd operational-state** [*group-id*] **Example:** `Device# show ip sla mpls-lsp-monitor lpd operational-state 100001`	(Optional) Displays the operational status of the LSP discovery groups belonging to an LSP Health Monitor operation. **Note** This command is applicable only if the LSP discovery option is enabled.
Step 7	**show ip sla mpls-lsp-monitor neighbors** **Example:** `Device# show ip sla mpls-lsp-monitor neighbors`	(Optional) Displays routing and connectivity information about MPLS VPN BGP next hop neighbors discovered by the LSP Health Monitor operation.
Step 8	**show ip sla mpls-lsp-monitor scan-queue** *operation-number* **Example:** `Device# show ip sla mpls-lsp-monitor scan-queue 1`	(Optional) Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an LSP Health Monitor operation.
Step 9	**show ip sla mpls-lsp-monitor summary** [*operation-number* [**group** [*group-id*]]] **Example:** `Device# show ip sla mpls-lsp-monitor summary`	(Optional) Displays BGP next hop neighbor and LSP discovery group information for LSP Health Monitor operations. **Note** This command is applicable only if the LSP discovery option is enabled.
Step 10	**show ip sla statistics** [*operation-number*] [**details**] **Example:** `Device# show ip sla statistics 100001`	(Optional) Displays the current operational status and statistics of all IP SLAs operations or a specified operation. **Note** This command applies only to manually configured IP SLAs operations.
Step 11	**show ip sla statistics aggregated** [*operation-number*] [**details**] **Example:** `Device# show ip sla statistics aggregated 100001`	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation. **Note** This command applies only to manually configured IP SLAs operations.

	Command or Action	Purpose
Step 12	**show mpls discovery vpn** **Example:** `Device# show mpls discovery vpn`	(Optional) Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

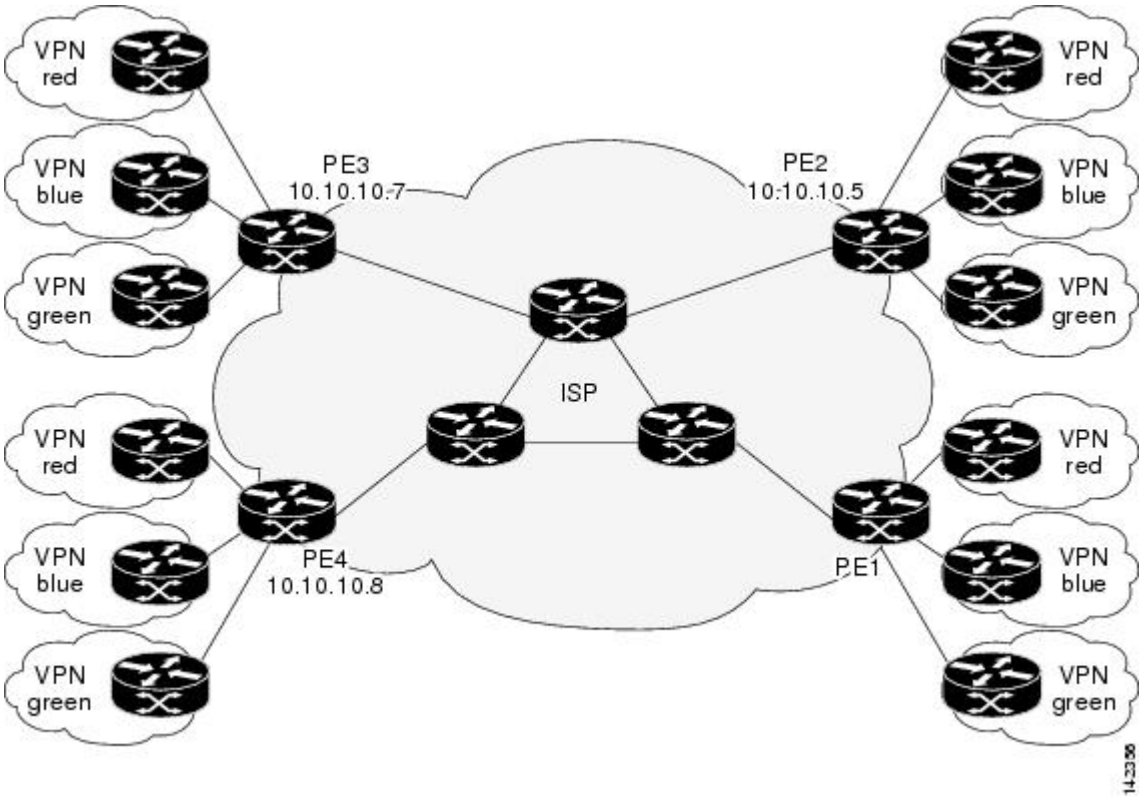
Configuration Examples for LSP Health Monitors

Example Configuring and Verifying the LSP Health Monitor Without LSP Discovery

The figure below illustrates a simple VPN scenario for an ISP. This network consists of a core MPLS VPN with four PE devices belonging to three VPNs: red, blue, and green. From the perspective of device PE1,

these VPNs are reachable remotely through BGP next hop devices PE2 (device ID: 10.10.10.5), PE3 (device ID: 10.10.10.7), and PE4 (device ID: 10.10.10.8).

Figure 7: Network Used for LSP Health Monitor Example



The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on PE1 (see the figure above) using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors (PE2, PE3, and PE4) in use by all VRFs (red, blue, and green) associated with device PE1. The BGP next hop neighbor process is enabled, and the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database is set to 60 seconds. The time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute. The secondary frequency option is enabled for both connection loss and timeout events, and the secondary frequency is set to 10 seconds. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss or timeout events occur, an SNMP trap notification is sent. Multioperation scheduling and the generation of IP SLAs SNMP system logging messages are enabled.

PE1 Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
```

```
 secondary-frequency both 10
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive
 3 action-type trapOnly
ip sla traps
snmp-server enable traps rtr
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

The following is sample output from the **show ip sla mpls-lsp-monitor configuration** command for PE1:

```
PE1# show ip sla mpls-lsp-monitor configuration 1
Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 1000
Threshold(ms)       : 5000
Frequency(sec)      : Equals schedule period
LSP Selector        : 127.0.0.1
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100001-100003
Schedule Period(sec): 60
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Secondary Frequency : Enabled on Timeout
         Value(sec) : 10
Reaction Configs    :
    Reaction        : connectionLoss
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
    Reaction        : timeout
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
```

The following is sample output from the **show mpls discovery vpn** command for PE1:

```
PE1# show mpls discovery vpn
Refresh interval set to 60 seconds.
Next refresh in 46 seconds
Next hop 10.10.10.5 (Prefix: 10.10.10.5/32)
        in use by: red, blue, green
Next hop 10.10.10.7 (Prefix: 10.10.10.7/32)
        in use by: red, blue, green
Next hop 10.10.10.8 (Prefix: 10.10.10.8/32)
        in use by: red, blue, green
```

The following is sample output from the **show ip sla mpls-lsp-monitor neighbors** command for PE1:

```
PE1# show ip sla mpls-lsp-monitor neighbors
IP SLA MPLS LSP Monitor Database : 1
BGP Next hop 10.10.10.5 (Prefix: 10.10.10.5/32)  OK
  ProbeID: 100001 (red, blue, green)
BGP Next hop 10.10.10.7 (Prefix: 10.10.10.7/32)  OK
  ProbeID: 100002 (red, blue, green)
BGP Next hop 10.10.10.8 (Prefix: 10.10.10.8/32)  OK
  ProbeID: 100003 (red, blue, green)
```

The following is sample output from the **show ip sla mpls-lsp-monitor scan-queue 1** and **debug ip sla mpls-lsp-monitor** commands when IP connectivity from PE1 to PE4 is lost. This output shows that connection loss to each of the VPNs associated with PE4 (red, blue, and green) was detected and that this information

was added to the LSP Health Monitor scan queue. Also, since PE4 is no longer a valid BGP next hop neighbor, the IP SLAs operation for PE4 (Probe 10003) is being deleted.

```
PE1# show ip sla mpls-lsp-monitor scan-queue 1
Next scan Time after: 20 Secs
Next Delete scan Time after: 20 Secs
BGP Next hop    Prefix            vrf                              Add/Delete?
10.10.10.8      0.0.0.0/0         red                              Del(100003)
10.10.10.8      0.0.0.0/0         blue                             Del(100003)
10.10.10.8      0.0.0.0/0         green                            Del(100003)
PE1# debug ip sla mpls-lsp-monitor
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:48: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf red from tree entry 10.10.10.8
*Aug 19 19:56: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:56: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf blue from tree entry 10.10.10.8
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf green from tree entry 10.10.10.8
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing Probe 100003
```

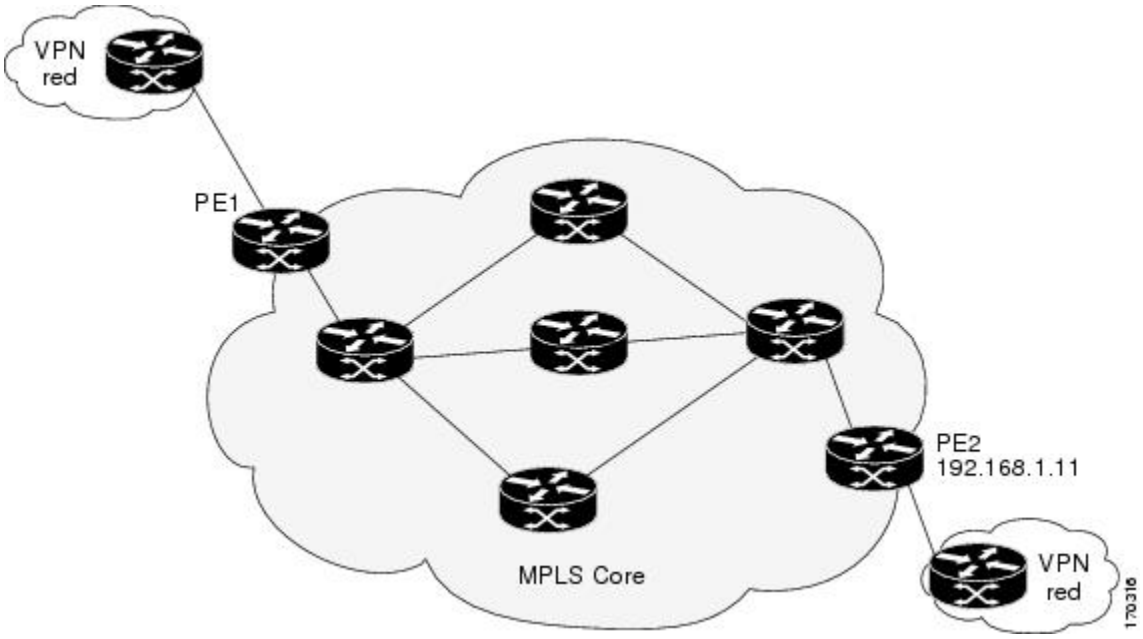
The following is sample output from the **show ip sla mpls-lsp-monitor scan-queue 1** and **debug ip sla mpls-lsp-monitor** commands when IP connectivity from PE1 to PE4 is restored. This output shows that each of the VPNs associated with PE4 (red, blue, and green) were discovered and that this information was added to the LSP Health Monitor scan queue. Also, since PE4 is a newly discovered BGP next hop neighbor, a new IP SLAs operation for PE4 (Probe 100005) is being created and added to the LSP Health Monitor multioperation schedule. Even though PE4 belongs to three VPNs, only one IP SLAs operation is being created.

```
PE1# show ip sla mpls-lsp-monitor scan-queue 1
Next scan Time after: 23 Secs
Next Delete scan Time after: 23 Secs
BGP Next hop    Prefix            vrf                              Add/Delete?
10.10.10.8      10.10.10.8/32     red                              Add
10.10.10.8      10.10.10.8/32     blue                             Add
10.10.10.8      10.10.10.8/32     green                            Add
PE1# debug ip sla mpls-lsp-monitor
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf red into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding Probe 100005
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding ProbeID 100005 to tree entry 10.10.10.8 (1)
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf blue into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf green into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Added Probe(s) 100005 will be scheduled after 26 secs over
 schedule period 60
```

Example Configuring and Verifying the LSP Health Monitor with LSP Discovery

The figure below illustrates a simple VPN scenario for an ISP. This network consists of a core MPLS VPN with two PE devices belonging to a VPN named red. From the perspective of device PE1, there are three equal-cost multipaths available to reach device PE2.

Figure 8: Network Used for LSP Health Monitor with LSP Discovery Example



The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on PE1 (see the figure above) using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 100. Operation 100 is configured to automatically create IP SLAs LSP ping operations for all equal-cost multipaths between PE1 and PE2. The BGP next hop neighbor process is enabled, and the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database is set to 30 seconds. The time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute. The secondary frequency option is enabled for both connection loss and timeout events, and the secondary frequency is set to 5 seconds. The explicit null label option for echo request packets is enabled. The LSP rediscovery time period is set to 3 minutes. As specified by the proactive threshold monitoring configuration, an SNMP trap notification will be sent when an LSP discovery group status changes occurs. Multioperation scheduling and the generation of IP SLAs SNMP system logging messages are enabled.

PE1 Configuration

```
mpls discovery vpn next-hop
mpls discovery vpn interval 30
!
auto ip sla mpls-lsp-monitor 100
 type echo ipsla-vrf-all
 scan-interval 1
 secondary-frequency both 5
!
```

```
 path-discover
 force-explicit-null
 scan-period 3
!
auto ip sla mpls-lsp-monitor reaction-configuration 100 react lpd-group retry 3 action-type
 trapOnly
!
auto ip sla mpls-lsp-monitor schedule 100 schedule-period 30 start-time now
!
ip sla logging traps
snmp-server enable traps rtr
```

The following is sample output from the **show ip sla mpls-lsp-monitor configuration** command for PE1:

```
PE1# show ip sla mpls-lsp-monitor configuration
Entry Number : 100
Modification time   : *21:50:16.411 GMT Tue Jun 20 2006
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 5000
Threshold(ms)       : 50
Frequency(sec)      : Equals schedule period
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100002
Schedule Period(sec): 30
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Path Discover       : Enable
    Maximum sessions          : 1
    Session Timeout(seconds)  : 120
    Base LSP Selector         : 127.0.0.0
    Echo Timeout(seconds)     : 5
    Send Interval(msec)       : 0
    Label Shimming Mode       : force-explicit-null
    Number of Stats Hours     : 2
    Scan Period(minutes)      : 3
Secondary Frequency : Enabled on Connection Loss and Timeout
         Value(sec) : 5
Reaction Configs    :
    Reaction        : Lpd Group
    Retry Number    : 3
    Action Type     : Trap Only
```

The following is sample output from the **show mpls discovery vpn** command for PE1:

```
PE1# show mpls discovery vpn
Refresh interval set to 30 seconds.
Next refresh in 4 seconds
Next hop 192.168.1.11 (Prefix: 192.168.1.11/32)
        in use by: red
```

The following is sample output from the **show ip sla mpls-lsp-monitor neighbors** command for PE1:

```
PE1# show ip sla mpls-lsp-monitor neighbors
IP SLA MPLS LSP Monitor Database : 100
BGP Next hop 192.168.1.11 (Prefix: 192.168.1.11/32)  OK Paths: 3
  ProbeID: 100001 (red)
```

The following is sample output from the **show ip sla mpls-lsp-monitor lpd operational-state** command for LSP discovery group 100001:

```
PE1# show ip sla mpls-lsp-monitor lpd operational-state
Entry number: 100001
MPLSLM Entry Number: 100
Target FEC Type: LDP IPv4 prefix
```

```
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :
Path   Outgoing   Lsp             Link  Conn  Adj             Downstream
Index  Interface  Selector        Type  Id    Addr            Label Stack     Status
1      Et0/0      127.0.0.8       90    0     10.10.18.30     21              OK
2      Et0/0      127.0.0.2       90    0     10.10.18.30     21              OK
3      Et0/0      127.0.0.1       90    0     10.10.18.30     21              OK
```

The following is sample output from the **show ip sla mpls-lsp-monitor collection-statistics** command for LSP discovery group 100001:

```
PE1# show ip sla mpls-lsp-monitor collection-statistics
Entry number: 100001
Start Time Index: *21:52:59.795 GMT Tue Jun 20 2006
Path Discovery Start Time: *22:08:04.507 GMT Tue Jun 20 2006
Target Destination IP address: 192.168.1.11
Path Discovery Status: OK
Path Discovery Completion Time: 3052
Path Discovery Minimum Paths: 3
Path Discovery Maximum Paths: 3
LSP Group Index: 100002
LSP Group Status: up
Total Pass: 36
Total Timeout: 0        Total Fail: 0
Latest Probe Status: 'up,up,up'
Latest Path Identifier: '127.0.0.8-Et0/0-21,127.0.0.2-Et0/0-21,127.0.0.1-Et0/0-21'
Minimum RTT: 280        Maximum RTT: 324        Average RTT: 290
```

The following is sample output from the **show ip sla mpls-lsp-monitor summary** command for LSP Health Monitor operation 100:

```
PE1# show ip sla mpls-lsp-monitor summary 100
Index                   -  MPLS LSP Monitor probe index
Destination             -  Target IP address of the BGP next hop
Status                  -  LPD group status
LPD Group ID            -  Unique index to identify the LPD group
Last Operation Time     -  Last time an operation was attempted by
                           a particular probe in the LPD Group
Index  Destination     Status     LPD Group ID    Last Operation Time
100    192.168.1.11    up         100001          *22:20:29.471 GMT Tue Jun 20 2006
```

The following is sample output from the **show ip sla mpls-lsp-monitor summary** command for LSP discovery group 100001:

```
PE1#show ip sla mpls-lsp-monitor summary 100 group 100001
Group ID                -  unique number to identify a LPD group
Lsp-selector            -  Unique 127/8 address used to identify a LPD
Last Operation status   -  Latest probe status
Last RTT                -  Latest Round Trip Time
Last Operation Time     -  Time when the last operation was attempted
Group ID  Lsp-Selector    Status     Failures    Successes   RTT   Last Operation Time
100001    127.0.0.8       up         0           55          320   *22:20:29.471 GMT Tue
Jun 20 2006
100001    127.0.0.2       up         0           55          376   *22:20:29.851 GMT Tue
Jun 20 2006
100001    127.0.0.1       up         0           55          300   *22:20:30.531 GMT Tue
Jun 20 2006
```

Example Manually Configuring an IP SLAs LSP Ping Operation

The following example shows how to manually configure and schedule an IP SLAs LSP ping operation:

```
ip sla 1
mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1
frequency 120
secondary-frequency timeout 30
!
ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type
 trapOnly
ip sla reaction-configuration 1 react timeout threshold-type consecutive 3 action-type
trapOnly
ip sla logging traps
!
ip sla schedule 1 start-time now life forever
```

Additional References

Related Documents

Related Topic	Document Title
MPLS LSP discovery management tool	"MPLS EM-MPLS LSP Multipath Tree Trace" chapter of the *Multiprotocol Label Switching Configuration Guide*
Configuring standard IP access lists	"Access Control Lists" chapter of the *Security Configuration Guide: Securing the Data Plane* guide
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" chapter of the *Cisco IOS P SLAs Configuration Guide*
Proactive threshold monitoring for IP SLAs	" Configuring Proactive Threshold Monitoring of IP SLAs Operations" chapter of the *Cisco IOS IP SLAs Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference

Standards

Standard	Title
draft-ietf-mpls-lsp-ping-09.txt	Detecting MPLS Data Plane Failures
draft-ietf-mpls-oam-frmwk-03.txt	A Framework for MPLS Operations and Management (OAM)

Standard	Title
draft-ietf-mpls-oam-requirements-06.txt	OAM Requirements for MPLS Networks

MIBs

MIB	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

RFCs

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

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

Related Topics

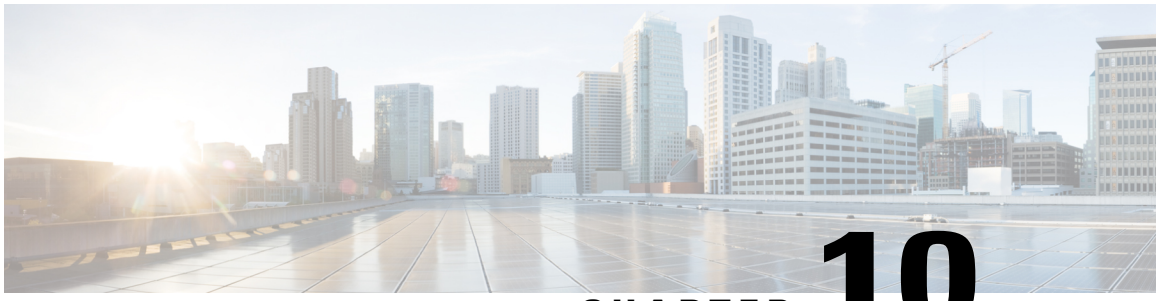
Feature Information for LSP Health Monitor Operations

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 21: Feature Information for the LSP Health Monitor

Feature Name	Releases	Feature Information
IP SLAs--LSP Health Monitor	12.4(6)T	The IP SLAs LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs.
IP SLAs--LSP Health Monitor		For software releases in which this feature was already introduced, new command-line interface (CLI) was implemented that replaces the CLI introduced in the earlier releases
IP SLAs--LSP Health Monitor with LSP Discovery		The LSP discovery capability was added.



CHAPTER 10

Configuring IP SLAs for Metro-Ethernet

This module describes how to configure an IP Service Level Agreements (SLAs) for Metro-Ethernet to gather network performance metrics in service-provider Ethernet networks. Available statistical measurements for the IP SLAs Ethernet operation include round-trip time, jitter (interpacket delay variance), and packet loss.

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.

Prerequisites for IP SLAs for Metro-Ethernet

It is recommended that the IEEE 802.1ag standard is supported on the destination devices in order to obtain complete error reporting and diagnostics information.

Restrictions for IP SLAs for Metro-Ethernet

- Memory and performance may be impacted for a given Ethernet CFM maintenance domain and Ethernet Virtual Circuit (EVC) or VLAN that has a large number of maintenance endpoints (MEPs).
- In case of PW redundancy, we need to have 2 different CFM/Y1731 sessions on active and backup PW. We cannot expect the same mpid and Y1731 session to work after PW switchover.
- Y1731 is not supported for port meps.
- CFM ans Y1731 is not supported for vpls cases, untagged EFP as well.

Information About IP SLAs for Metro-Ethernet

IP SLAs Ethernet Operation Basics

The IP SLAs for Metro-Ethernet integrates IP SLAs with the Ethernet Connectivity Fault Management (CFM) feature. Ethernet CFM is an end-to-end per-service-instance Ethernet-layer operation, administration, and management (OAM) protocol.

The IP SLAs for Metro-Ethernet feature provides the capability to gather statistical measurements by sending and receiving Ethernet data frames between Ethernet CFM maintenance endpoints (MEPs). The performance metrics for IP SLAs Ethernet operations are measured between a source MEP and a destination MEP. Unlike existing IP SLAs operations that provide performance metrics for the IP layer, the IP SLAs Ethernet operation provides performance metrics for Layer 2.

IP SLAs Ethernet operations may be configured using the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

You can manually configure individual Ethernet ping or Ethernet jitter operations by specifying the destination MEP identification number, name of the maintenance domain, and EVC or VLAN identifier or port level option.

You also have the option to configure an IP SLAs auto Ethernet operation (ping or jitter) that will query the Ethernet CFM database for all maintenance endpoints in a given maintenance domain and EVC or VLAN. When an IP SLAs auto Ethernet operation is configured, individual Ethernet ping or Ethernet jitter operations are automatically created based on the MEPs that were discovered. A notification mechanism exists between the IP SLAs and Ethernet CFM subsystems to facilitate the automatic creation of Ethernet ping or Ethernet jitter operations for applicable MEPs that are added to a given maintenance domain and EVC or VLAN while an auto Ethernet operation is running.

The IP SLAs for Metro-Ethernet feature supports multioperation scheduling of IP SLAs operations and proactive threshold violation monitoring through SNMP trap notifications and syslog messages.

Statistics Measured by the IP SLAs Ethernet Operation

The network performance metrics supported by the IP SLAs Ethernet operation is similar to the metrics supported by existing IP SLAs operations. The statistical measurements supported by the IP SLAs Ethernet jitter operation include the following:

- Round-trip time latency

- Unprocessed packets
- Packet loss (source-to-destination and destination-to-source)
- Out-of-sequence, tail-dropped, and late packets

How to Configure IP SLAs for Metro-Ethernet

Note There is no need to configure an IP SLAs responder on the destination device.

Configuring an IP SLAs Auto Ethernet Operation with Endpoint Discovery on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla ethernet-monitor** *operation-number*
4. **type echo domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*]
5. **type jitter domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*] [**interval** *interframe-interval*] [**num-frames** *frames-number*]
6. **cos** *cos-value*
7. **owner** *owner-id*
8. **request-data-size** *bytes*
9. **tag** *text*
10. **threshold** *milliseconds*
11. **timeout** *milliseconds*
12. **end**
13. **show ip sla ethernet-monitor 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 ethernet-monitor** *operation-number* **Example:** `Device(config)# ip sla ethernet-monitor 1`	Begins configuration for an IP SLAs auto Ethernet operation and enters IP SLA Ethernet monitor configuration mode.
Step 4	**type echo domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*] **Example:** `Device(config-ip-sla-ethernet-monitor)# type echo domain testdomain vlan 34`	• **domain** *domain-name*—Specify the name of the created domain. • **vlan***vlan-id*—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma. • **exclude-mpids***mp-ids*—Enter a maintenance end point identifier (mpid). The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. For Echo operations only: Configures an auto Ethernet operation for Ethernet ping operations. **Note** Depending on your release, the **evc** *evc-id* keyword and argument combination may not be available for this command.
Step 5	**type jitter domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*] [**interval** *interframe-interval*] [**num-frames** *frames-number*] **Example:** `Device(config-ip-sla-ethernet-monitor)# type jitter domain testdomain evc testevc interval 20 num-frames 30`	For Jitter operations only: Configures an auto Ethernet operation for Ethernet jitter operations. **Note** Depending on your release, the **evc** *evc-id* keyword and argument combination may not be available for this command.
Step 6	**cos** *cos-value* **Example:** `Device(config-ip-sla-ethernet-params)# cos 2`	(Optional) Sets the class of service for an IP SLAs Ethernet operation.
Step 7	**owner** *owner-id* **Example:** `Device(config-ip-sla-ethernet-params)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.

	Command or Action	Purpose
Step 8	**request-data-size** *bytes* **Example:** `Device(config-ip-sla-ethernet-params)# request-data-size 64`	(Optional) Sets the padding size for the data frame of an IP SLAs Ethernet operation. • The default value for IP SLAs Ethernet ping operations is 66 bytes. • The default value for IP SLAs Ethernet jitter operations is 51 bytes.
Step 9	**tag** *text* **Example:** `Device(config-ip-sla-ethernet-params)# tag TelnetPollSever1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 10	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-ethernet-params)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 11	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-ethernet-params)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 12	**end** **Example:** `Device(config-ip-sla-ethernet-params)# end`	Exits to privileged EXEC configuration mode.
Step 13	**show ip sla ethernet-monitor configuration** [*operation-number*] **Example:** `Device# show ip sla ethernet-monitor configuration 1`	(Optional) Displays configuration settings for all IP SLAs auto Ethernet operations or a specified auto Ethernet operation.

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.

Manually Configuring an IP SLAs Ethernet Ping or Jitter Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet echo mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*}
5. **ethernet jitter mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} [**interval** *interframe-interval*] [**num-frames** *frames-number*]
6. **cos** *cos-value*
7. **frequency** *seconds*
8. **history** *history-parameter*
9. **owner** *owner-id*
10. **request-data-size** *bytes*
11. **tag** *text*
12. **threshold** *milliseconds*
13. **timeout** *milliseconds*
14. **end**
15. **show ip sla configuration** [*operation-number*]
16. **show ip sla application**

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 1`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	**ethernet echo mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} **Example:** `Device(config-ip-sla)# ethernet echo mpid 23 domain testdomain vlan 34`	For a ping operation only: Configures the IP SLAs operation as an Ethernet ping operation and enters Ethernet echo configuration mode. **Note** Depending on your release, the **evc** evc-id keyword and argument combination may not be available for this command.
Step 5	**ethernet jitter mpid** *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} [**interval** *interframe-interval*] [**num-frames** *frames-number*] **Example:** `Device(config-ip-sla)# ethernet jitter mpid 23 domain testdomain evc testevc interval 20 num-frames 30`	For a jitter operation only: Configures the IP SLAs operation as an Ethernet jitter operation and enters Ethernet jitter configuration mode. **Note** Depending on your release, the **evc** evc-id keyword and argument combination may not be available for this command.
Step 6	**cos** *cos-value* **Example:** `Device(config-ip-sla-ethernet-echo)# cos 2`	(Optional) Sets the class of service for an IP SLAs Ethernet operation. **Note** For this and the remaining steps, the configuration mode shown in the example is for configuring an Ethernet echo operation. However, the commands are the same in the Ethernet jitter configuration mode.
Step 7	**frequency** *seconds* **Example:** `Device(config-ip-sla-ethernet-echo)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 8	**history** *history-parameter* **Example:** `Device(config-ip-sla-ethernet-echo)# history hours-of-statistics-kept 3`	(Optional) Specifies the parameters used for gathering statistical history information for an IP SLAs operation.
Step 9	**owner** *owner-id* **Example:** `Device(config-ip-sla-ethernet-echo)# 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-ethernet-echo)# request-data-size 64`	(Optional) Sets the padding size for the data frame of an IP SLAs Ethernet operation. The default value for IP SLAs Ethernet ping operations is 66 bytes. The default value for IP SLAs Ethernet jitter operations is 51 bytes.

	Command or Action	Purpose
Step 11	**tag** *text* **Example:** `Device(config-ip-sla-ethernet-echo)# tag TelnetPollSever1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 12	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-ethernet-echo)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 13	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-ethernet-echo)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 14	**end** **Example:** `Device(config-ip-sla-ethernet-echo)# end`	Exits to privileged EXEC mode.
Step 15	**show ip sla configuration** [*operation-number*] **Example:** `Device# show ip sla configuration 1`	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.
Step 16	**show ip sla application** **Example:** `Device# show ip sla application`	(Optional) Displays global information about supported IP SLAs features.

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

Note

- All IP SLAs operations to be scheduled must be already configured.
- The frequency of all operations scheduled in an operation group must be the same unless you are enabling the random scheduler option for a multioperation scheduler.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ip sla ethernet-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* **:** *mm* **:** *ss* | *hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **now** | **pending**}]
   - **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* [**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. **exit**
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	Do one of the following: • **ip sla ethernet-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time**	• The first example shows how to configure scheduling parameters for an IP SLAs auto Ethernet operation.

	Command or Action	Purpose

	{**after** *hh* **:** *mm* **:** *ss* | *hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **now** | **pending**}]
	• **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* [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]
	Example:
	`Device(config)# ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now`
	`Device(config)# ip sla schedule 1 start-time now life forever`
	`Device(config)# ip sla group schedule 1 3,4,6-9`
		• The second example shows how to configure the scheduling parameters for an individual IP SLAs operation.
		• The third example shows how to specifiy an IP SLAs operation group number and range of operation numbers to be scheduled for a multioperation scheduler.

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

Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs Ethernet ping or Ethernet jitter operation. Use the **debug ip sla ethernet-monitor** command to help troubleshoot issues with an IP SLAs auto Ethernet operation.

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.

operation)

To display and interpret the results of an IP SLAs operation, use the **show ip sla statistics** command. Check the output for fields that correspond to criteria in your service level agreement to determine whether the service metrics are acceptable.

Configuration Examples for IP SLAs for Metro-Ethernet

Example IP SLAs Auto Ethernet Operation with Endpoint Discovery

The following examples shows the operation parameters, proactive threshold monitoring, and scheduling options for an IP SLAs auto Ethernet operation. In Configuration A, operation 10 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance endpoints in the domain named testdomain and VLAN identification number 34. In Configuration B, operation 20 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance endpoints in the domain named testdomain and EVC identified as testevc. In both configurations, the proactive threshold monitoring configuration specifies that when three consecutive connection loss events occur, an SNMP trap notification should be sent. The schedule period for operation 10 and operation 20 is 60 seconds, and both operations are scheduled to start immediately.

Configuration A

```
ip sla ethernet-monitor 10
 type echo domain testdomain vlan 34
!
ip sla ethernet-monitor reaction-configuration 10 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

Configuration B

```
ip sla ethernet-monitor 20
 type echo domain testdomain evc testevc
!
ip sla ethernet-monitor reaction-configuration 20 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 20 schedule-period 60 start-time now
```

Example Individual IP SLAs Ethernet Ping Operation

The following example show the configuration for an IP SLAs Ethernet ping operation. In Configuration C, the maintenance endpoint identification number is 23, the maintenance domain name is testdomain, and the VLAN identification number is 34. In Configuration D, the maintenance endpoint identification number is 23, the maintenance domain name is testdomain, and the EVC is identified as testevc. In both configurations,

the proactive threshold monitoring configuration specifies that when three consecutive connection loss events occur, an SNMP trap notification should be sent. Operation 1 and operation 5 are scheduled to start immediately.

Configuration C

```
ip sla 1
 ethernet echo mpid 23 domain testdomain vlan 34
!
ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type
 trapOnly
!
ip sla schedule 1 start-time now
```

Configuration D

```
ip sla 5
 ethernet echo mpid 23 domain testdomain evc testevc
!
ip sla reaction-configuration 5 react connectionLoss threshold-type consecutive 3 action-type
 trapOnly
!
ip sla schedule 5 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, All Releases
Cisco IOS IP SLAs: general information	"Cisco IOS IP SLAs Overview" module of the *Cisco IOS IP SLAs Configuration Guide*.
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" module of the *Cisco IOS P SLAs Configuration Guide*
Proactive threshold monitoring for IP SLAs	"Configuring Proactive Threshold Monitoring of IP SLAs Operations" module of the *Cisco IOS IP SLAs Configuration Guide*

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 IP SLAs for Metro-Ethernet

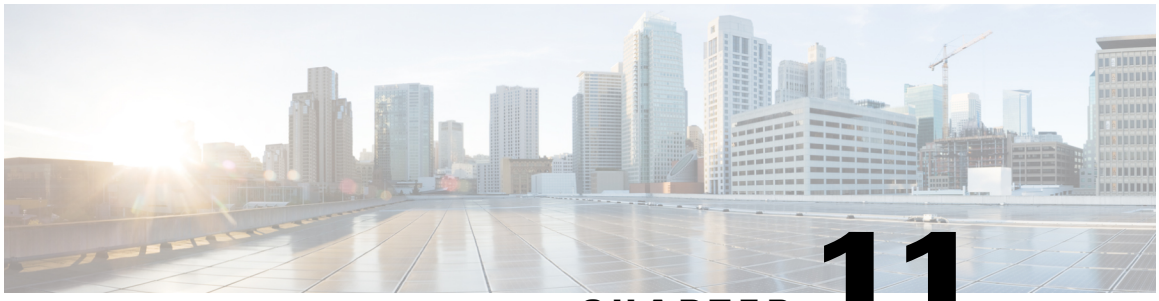
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 22: Feature Information for IP SLAs for Metro-Ethernet

Feature Name	Releases	Feature Information
IP SLAs for Metro-Ethernet	12.4(20)T	The IP Service Level Agreements (SLAs) for Metro-Ethernet feature provides the capability to gather Ethernet-layer network performance metrics. Available statistical measurements for the IP SLAs Ethernet operation include round-trip time, jitter (interpacket delay variance), and packet loss.
IP SLAs Metro-Ethernet 2.0 (EVC)		Support for Ethernet Virtual Circuits (EVCs) was added.

Feature Name	Releases	Feature Information
IP SLAs Metro-Ethernet 3.0 (CFM d8.1)		Support for the Standards Based EOAM Performance Monitoring CFM base feature was added. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 900 Series.



CHAPTER 11

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

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

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 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`	

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.

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 *Cisco IOS IP SLAs Configuration Guide*.

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
• 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	*Internet Control Message Protocol*

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

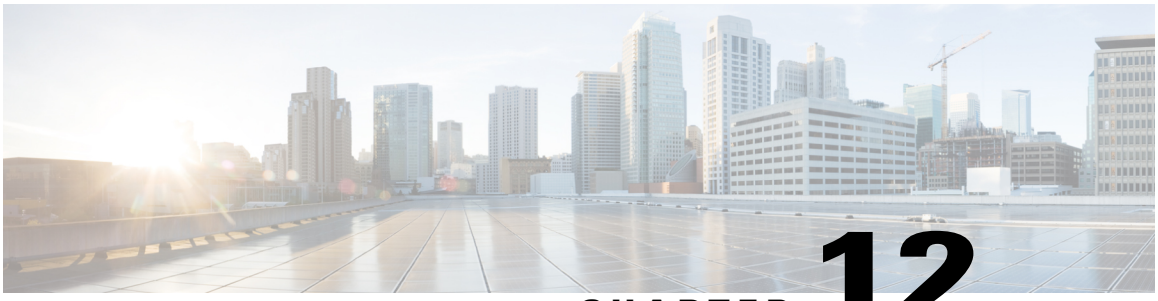
Feature Information for IP SLAs - ICMP Jitter Operation

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 23: Feature Information for IP SLAs - ICMP Jitter Operation

Feature Name	Releases	Feature Information
IP SLAs ICMP Jitter Operation		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.



CHAPTER 12

Configuring RTP-Based VoIP Operations

This module describes how to configure an IP Service Level Agreements (SLAs) Real-Time Transport Protocol (RTP)-based Voice over IP (VoIP) Operation feature to set up and schedule a test call for using Voice gateway digital signal processors (DSPs) to gather network performance-related statistics for the call. Available statistical measurements for VoIP networks include jitter, frame loss, Mean Opinion Score for Conversational Quality (MOS-CQ), and Mean Opinion Score for Listening Quality (MOS-LQ).

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.

Prerequisites for IP SLAs RTP-Based VoIP Operations

- Both the source and destination routers must be running Cisco IOS Release 12.4(4)T or later releases.

- Both the source and destination routers must be running a Cisco IOS image with the Cisco IOS IP Voice or higher grade feature package.
- The source router must have a network module with a c5510 or c549 DSP. The destination router need not have a network module with a DSP.
- The IP SLAs Responder must be enabled on the destination gateway.

Restrictions for IP SLAs RTP-Based VoIP Operations

- The IP SLAs RTP-based VoIP operation gathers statistical information only from the DSP of the source router.
- For source-to-destination measurements, the RTP-based VoIP operation does not obtain statistical information from DSPs.
- Depending on the type of DSP, the statistics measured by the IP SLAs RTP-based VoIP operation will vary. For more information, see the "Statistics Measured by the IP SLAs RTP-Based VoIP Operation" section.
- The voice port used by the IP SLAs RTP-based VoIP operation will not be available for other calls.

Information About IP SLAs RTP-Based VoIP Operations

Benefits of the IP SLAs RTP-Based VoIP Operation

The IP SLAs RTP-Based VoIP Operation feature provides the following key benefits:

- End-to-end performance measurements using DSPs for determining voice quality in VoIP networks.
- Proactive threshold violation monitoring through Simple Network Management Protocol (SNMP) trap notifications and syslog messages.

Statistics Measured by the IP SLAs RTP-Based VoIP Operation

The IP SLAs RTP-based VoIP operation provides an enhanced capability to measure voice quality using DSP-based calculations to determine MOS scores. For customer scenarios where the destination gateway does not have DSP hardware, statistical information is gathered only from the DSP of the source gateway. In this case, the RTP data stream is looped back from the destination to the source gateway.

The statistics gathered by the IP SLAs RTP-based VoIP operation will vary depending on the type of DSP module (see the tables below).

Table 24: Statistics Gathered by the RTP-Based VoIP Operation for c549 DSPs

Statistics	Description
Interarrival jitter (destination-to-source and source-to-destination)	Interarrival jitter is the mean deviation (smoothed absolute value) of the difference in packet spacing for a pair of packets. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement. For more information about interarrival jitter, see RFC 3550 (*RTP: A Transport Protocol for Real-Time Applications*).
Estimated R factor (destination-to-source and source-to-destination)	Estimated transmission rating factor R. This value is based on one-way transmission delay and standard default values. No values are obtained from the DSP to calculate the estimated transmission rating factor R. For more information about the estimated R factor, see International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation G.107 (*The E-model, a computational model for use in transmission planning*).
MOS-CQ (destination-to-source and source-to-destination)	Mean Opinion Score for Conversational Quality. This value is obtained by conversion of the estimated R factor to Mean Opinion Score (MOS) using ITU-T Recommendation G.107 conversion tables. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement.
Round-trip time (RTT) latency	Round-trip time latency for an RTP packet to travel from the source to the destination and back to the source.
Packet loss (destination-to-source and source-to-destination)	Number of packets lost. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement.

Statistics	Description
Packets missing in action (source-to-destination)	Number of missing packets. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement.
One-way latency (destination-to-source and source-to-destination)	Average, minimum, and maximum latency values. These values are measured by sending RTP packets to IP SLAs Responder. The RTP data stream is then looped back from the destination to the source gateway.

Table 25: Statistics Gathered by the RTP-Based VoIP Operation for c5510 DSPs

Statistics	Description
Interarrival jitter (destination-to-source and source-to-destination)	Interarrival jitter is the mean deviation (smoothed absolute value) of the difference in packet spacing for a pair of packets. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement. For more information on how this value is calculated, see RFC 1889 (*RTP: A Transport Protocol for Real-Time Applications*).
Estimated R factor (destination-to-source and source-to-destination)	Estimated transmission rating factor R. This value is based on one-way transmission delay and standard default values, as well as values obtained from the DSP. For more information about how to calculate the estimated R factor, see International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation G.107 (*The E-model, a computational model for use in transmission planning*).

Statistics	Description
MOS-CQ (destination-to-source and source-to-destination)	Mean Opinion Score for Conversational Quality. This value is obtained by conversion of the estimated R factor to Mean Opinion Score (MOS) using ITU-T Recommendation G.107 conversion tables. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement.
Round-trip time (RTT) latency	Round-trip time latency for an RTP packet to travel from the source to the destination and back to the source.
Packet loss (destination-to-source and source-to-destination)	Number of packets lost. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement.
Packets missing in action (source-to-destination)	Number of missing packets. The source-to-destination value is measured by sending RTP packets to the IP SLAs Responder. No values are obtained from the DSP for this measurement.
One-way latency (destination-to-source and source-to-destination)	Average, minimum, and maximum latency values. These values are measured by sending RTP packets to IP SLAs Responder. The RTP data stream is then looped back from the destination to the source gateway.
Frame loss (destination-to-source)	Number of DSP frame loss events. A frame loss can occur due to such events as packet loss, late packets, or a jitter buffer error.
MOS-LQ (destination-to-source)	Mean Opinion Score for Listening Quality.

How to Configure IP SLAs RTP-Based VoIP Operations

Configuring and Scheduling an IP SLAs RTP-Based VoIP Operation

Perform this task to configure and schedule an IP SLAs RTP-based VoIP operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **voip rtp** {*destination-ip-address* | *destination-hostname*} **source-ip** {*ip-address* | *hostname*} **source-voice-port** {*slot* [/ *subunit* / *port* **:** *ds0-group-number*]} [**codec** *codec-type*] [**duration** *seconds*] [**advantage-factor** *value*]
5. **frequency** *seconds*
6. **history** *history-parameter*
7. **owner** *text*
8. **tag** *text*
9. **threshold** *milliseconds*
10. **timeout** *milliseconds*
11. **exit**
12. **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]
13. **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**]
14. **exit**
15. **show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 1`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	**voip rtp** {*destination-ip-address* | *destination-hostname*} **source-ip** {*ip-address* | *hostname*} **source-voice-port** {*slot* [/ *subunit* / *port* **:** *ds0-group-number*]} [**codec** *codec-type*] [**duration** *seconds*] [**advantage-factor** *value*] **Example:** `Router(config-ip-sla)# voip rtp 10.2.3.4 source-ip 10.5.6.7 source-voice-port 1/0:1 codec g711alaw duration 30 advantage-factor 5`	Enters IP SLAs VoIP RTP configuration mode and configures the IP SLAs operation as an RTP-based VoIP operation.
Step 5	**frequency** *seconds* **Example:** `Router(config-ip-sla-voip-rtp)# frequency 90`	(Optional) Sets the rate at which a specified IP SLAs operation repeats. The default frequency value is 60 seconds.
Step 6	**history** *history-parameter* **Example:** `Router(config-ip-sla-voip-rtp)# history buckets-kept 25`	(Optional) Specifies the parameters used for gathering statistical history information for an IP SLAs operation.
Step 7	**owner** *text* **Example:** `Router(config-ip-sla-voip-rtp)# owner 10.16.1.1 cwb.cisco.com John Doe RTP 555-1212`	(Optional) Configures the SNMP owner of an IP SLAs operation.
Step 8	**tag** *text* **Example:** `Router(config-ip-sla-voip-rtp)# tag testoperation`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	**threshold** *milliseconds* **Example:** `Router(config-ip-sla-voip-rtp)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 10	**timeout** *milliseconds* **Example:** `Router(config-ip-sla-voip-rtp)# 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 11	**exit** **Example:** `Router(config-ip-sla-voip-rtp)# exit`	Exits IP SLAs VoIP RTP configuration submode and returns to global configuration mode.
Step 12	**ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*] **Example:** `Router(config)# ip sla reaction-configuration 1 react frameLossDS action-type traponly threshold-type consecutive 3`	(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.
Step 13	**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:** `Router(config)# ip sla schedule 1 start-time now life forever`	Specifies the scheduling parameters for an IP SLAs operation.
Step 14	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.
Step 15	**show ip sla configuration** [*operation-number*] **Example:** `Router# show ip sla configuration 10`	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Troubleshooting Tips

- If the IP SLAs operation is not running and not 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 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 view and interpret the results of an IP SLAs operation use the **show ip sla statistics** and **show ip sla statistics aggregated**commands. 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 Examples for IP SLAs RTP-Based VoIP Operations

Example Configuring an IP SLAs RTP-Based VoIP Operation

The following example shows how to configure an IP SLAs RTP-based VoIP operation:

```
ip sla 1
 voip rtp 10.2.3.4 source-ip 10.5.6.7 source-voice-port 1/0:1 codec g711alaw duration 30
advantage-factor 5
!
ip sla reaction-configuration 1 react FrameLossDS action-type traponly threshold-type
consecutive 3
!
ip sla schedule 1 start-time now life forever
```

Use the **show ip sla statistics** command in privileged EXEC mode to display the current operational status and statistics for an IP SLAs operation. Use the **show ip sla statistics aggregated** command in privileged EXEC mode to display the aggregated hourly status and statistics for an IP SLAs operation.

Additional References

The following sections provide references related to the IP SLAs RTP-Based VoIP Operation feature.

Related Documents

Related Topic	Document Title
Cisco IOS IP SLAs UDP-based VoIP operations for VoIP networks	Configuring UDP Jitter Operations for VoIP chapter of the *Cisco IOS IP SLAs Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	*Cisco IOS IP SLAs Command Reference*

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
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

RFCs

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

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

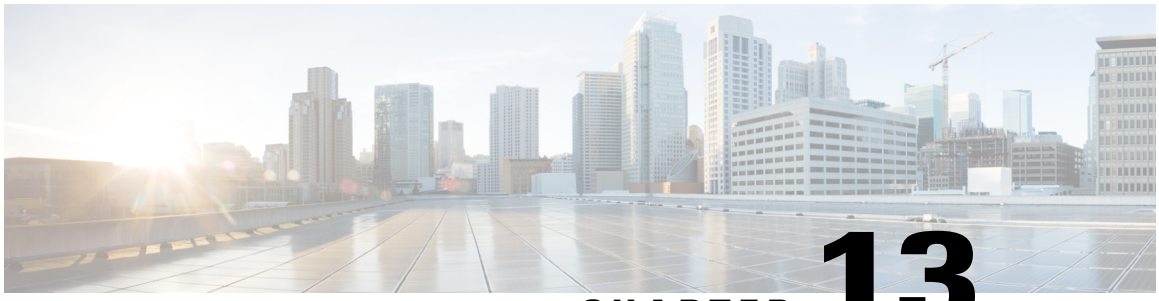
Feature Information for IP SLAs RTP-Based VoIP Operations

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 26: Feature Information for IP SLAs RTP-Based VoIP Operations

Feature Name	Releases	Feature Information
IP SLAs RTP-Based VoIP Operation	12.4(4)T	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 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 between a Cisco device (source) and any other IP device (destination).
IP SLAs RTP-Based VoIP Operation Enhancements	12.4(6)T	New statistical measurement options for the source-to-destination data path were added.



CHAPTER 13

Configuring VoIP Gatekeeper Registration Delay Operations

This document describes how to configure an Cisco IOS IP Service Level Agreements (SLAs) Voice over IP (VoIP) gatekeeper registration delay operation to determine the average, median, or aggregated response time (delay) of registration attempts from a VoIP gateway to a VoIP gatekeeper device.

To measure VoIP gatekeeper registration response time, the gatekeeper registration delay operation functions by sending a lightweight Registration Request (RRQ) from an H.323 gateway (GW) to an H.323 gatekeeper (GK), and recording the amount of time taken to receive the Registration Confirmation (RCF) back from the gatekeeper.

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 VoIP Gatekeeper Registration Delay Operations

You cannot configure the IP SLAs VoIP gatekeeper registration delay operation if the gatekeeper has already been registered with the gateway.

Information About IP SLAs VoIP Gatekeeper Registration Delay Operations

H.323 Gatekeepers and Gateways

H.232 is the ITU-T protocol standard used for managing and facilitating packetized voice and video over local-area networks (LANs, particularly intranets) and over the Internet. H.323 consists of several component standards; see the “Glossary” section of this chapter for details on these standardized protocols.

H.323 is considered an “umbrella protocol” because it defines all aspects of call transmission, from call establishment to capabilities exchange to network resource availability. H.323 defines Registration, Admission, and Status (RAS) protocols for call routing, H.225 protocols for call setup, and H.245 protocols for capabilities exchange. The IP SLAs VoIP Gatekeeper Registration Delay Monitoring feature focuses on the function of the call control H.323 stack.

For an in-depth discussion of H.323, including gatekeeper and gateway functionality, see the “H.323 Applications” chapter of the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

Gateway-to-Gatekeeper Registration Delay Time Monitoring

The IP SLAs VoIP gatekeeper registration delay operation provides statistical data on the amount of time taken to register a gateway to a gatekeeper. IP SLAs was designed to gather information over time, at intervals you specify, so that statistics can be provided on key metrics often used in Service Level Agreements (SLAs). Aggregated totals, median, or average data can be viewed using the Cisco IOS command-line interface (CLI) on the device running IP SLAs, or retrieved from the device by external applications using SNMP.

Cisco IOS IP SLAs also provides notification options based on performance thresholds and reaction triggering. These notification options allow for proactive monitoring in an environment where IT departments can be alerted to potential network problems, rather than having to manually examine data.

This operation will measure time from when the RRQ message is sent and when RCF message is received. A timeout may be required if a response is not received in a certain timeframe.

How to Configure IP SLAs VoIP Gatekeeper Registration Delay Operations

Configuring the VoIP H.323 Gateway

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gateway**
4. **exit**
5. **interface** *interface-id*
6. **ip address** *ip-address subnet-mask*
7. **h323-gateway voip interface**
8. **h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**}
9. **h323-gateway voip h323-id** *interface-id*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**gateway** **Example:** `Router(config)# gateway`	Enables the H.323 VoIP gateway and enters gateway configuration mode.
Step 4	**exit** **Example:** `Router(config-gateway)# exit`	Exits gateway configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 5	**interface** *interface-id* **Example:** `Router(config)# interface Ethernet1/1`	Specifies an interface and enters interface configuration mode.
Step 6	**ip address** *ip-address subnet-mask* **Example:** `Router(config-if)# ip address 172.29.129.123 255.255.255.0`	Configures the IP address of the interface.
Step 7	**h323-gateway voip interface** **Example:** `Router(config-if)# h323-gateway voip interface`	Configures the interface as an H.323 gateway interface.

Step 8	**h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**}
	
	Example:
	[**priority** *number*]
	
	Example:
	`Router(config-if)# h323-gateway voip id zone1 ipaddr 172.29.129.124 1719`
	
	Example:
	`Router(config-if)# h323-gateway voip id saagk ipaddr 172.29.129.28 1719`
		Defines the name and location of the gatekeeper for a specific gateway.
		• Repeat this step for each ID (see example).

Step 9	**h323-gateway voip h323-id** *interface-id* **Example:** `Router(config-if)# h323-gateway voip h323-id GWZ`	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
Step 10	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Example

The following example shows sample output from the **show gateway** command if the gateway (named GW3) is registered to a gatekeeper (named slagk):

```
Router# show gateway
H.323 ITU-T Version: 4.0   H323 Stack Version: 0.1
 H.323 service is up
 Gateway  GW3 is registered to Gatekeeper slagk
Alias list (CLI configured)
 E164-ID 2073418
 E164-ID 5251212
 H323-ID GW3
Alias list (last RCF)
 E164-ID 2073418
 E164-ID 5251212
 H323-ID GW3
    H323 resource thresholding is Disabled
```

The following example shows sample output for the **show gateway** command if the gateway is not registered to a gatekeeper:

```
Router# show gateway
 Gateway gw3 is not registered to any gatekeeper
Alias list (CLI configured)
 E164-ID 2073418
 E164-ID 5251212
 H323-ID gw3/ww
Alias list (last RCF)
    H323 resource thresholding is Disabled
```

Use the**show gatekeeper endpoint** command to verify the endpoint's registration status to the gatekeeper. The following example shows the common output of this command if an endpoint is registered:

```
Router# show gatekeeper endpoint
            GATEKEEPER ENDPOINT REGISTRATION
            ================================
CallSignalAddr   Port   RASSignalAddr   Port   Zone Name   Type   Flags
--------------   -----  -------------   ----   ---------   ----   -----
172.16.13.35     1720   172.16.13.35    50890  gk          VOIP-GW
    E164-ID: 2073418
    E164-ID: 5251212
    H323-ID: gw3
   Total number of active registrations = 1
```

The following example shows the common output of the **show gatekeeper endpoint** command if an endpoint is not registered:

```
Router# show gatekeeper endpoint
            GATEKEEPER ENDPOINT REGISTRATION
            ================================
CallSignalAddr   Port   RASSignalAddr   Port   Zone Name   Type   Flags
--------------   -----  -------------   ----   ---------   ----   -----
   Total number of active registrations = 0
```

The following configuration example shows a properly configured gateway:

```
gateway
interface Ethernet1/1
 ip address 172.29.129.123 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id zone1 ipaddr 172.29.129.124 1719
 h323-gateway voip id saagk ipaddr 172.29.129.28 1719
 h323-gateway voip h323-id GWZ
```

Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs LSP ping or LSP traceroute operation.

Configuring and Scheduling a VoIP Gatekeeper Registration Delay Operation

Before You Begin

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **voip delay gatekeeper-registration**
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **verify-data**
18. **exit**
19. **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**]
20. **exit**
21. **show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**voip delay gatekeeper-registration** **Example:** `Router(config-ip-sla)# voip delay gatekeeper-registration`	Configures the IP SLAs operation as a VoIP gatekeeper registration delay operation and enters IP SLA VoIP configuration mode. • If the gatekeeper has not been registered with the gateway prior to entering this command, the following error message will be displayed: No gatekeeper has been registered!
Step 5	**history buckets-kept** *size* **Example:** `Router(config-ip-sla-voip)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-ip-sla-voip)# 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:** `Router(config-ip-sla-voip)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-ip-sla-voip)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.

	Command or Action	Purpose
Step 9	**frequency** *seconds* **Example:** `Router(config-ip-sla-voip)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-ip-sla-voip)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	**history lives-kept** *lives* **Example:** `Router(config-ip-sla-voip)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	**owner** *owner-id* **Example:** `Router(config-ip-sla-voip)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-ip-sla-voip)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	**tag** *text* **Example:** `Router(config-ip-sla-voip)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	**threshold** *milliseconds* **Example:** `Router(config-ip-sla-voip)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	**timeout** *milliseconds* **Example:** `Router(config-ip-sla-voip)# 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 17	**verify-data** **Example:** `Router(config-ip-sla-voip)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 18	**exit** **Example:** `Router(config-ip-sla-voip)# exit`	Exits VoIP configuration submode and returns to global configuration mode.
Step 19	**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:** **Example:** `Router(config)# ip sla schedule 5 start-time now life forever`	Configures the scheduling parameters for an individual IP SLAs operation.
Step 20	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.
Step 21	**show ip sla configuration** [*operation-number*] **Example:** `Router# show ip sla configuration 10`	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Troubleshooting Tips

- If the IP SLAs operation is not running and not 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 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 SLAs operation, see the “Configuring Proactive Threshold Monitoring” section.

operation)

To display and interpret the results of an IP SLAs operation, use the **show ip sla statistics** command. Check the output for fields that correspond to criteria in your service level agreement to determine whether the service metrics are acceptable.

Configuration Examples for IP SLAs VoIP Gatekeeper Registration Delay Operations

Example Configuring the IP SLAs VoIP gatekeeper registration delay operation

In the following example, a VoIP gatekeeper registration delay operation is configured and scheduled to start immediately. This example assumes the gateway to gatekeeper relationship has already been configured.

```
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# voip delay gatekeeper-registration
Router(config-ip-sla-voip)# exit
Router(config)# ip sla schedule 1 start-time now life forever
```

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*
Gateway and gatekeeper configuration using Cisco IOS Release 12.3 and later releases	*Cisco IOS Voice Configuration Library*
Troubleshooting gatekeeper configurations	Troubleshooting Gatekeeper Registration Issues

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
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

RFCs

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

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 VoIP Gatekeeper Registration Delay 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 27: Feature Information for IP SLAs VoIP Gatekeeper Registration Delay Operations

Feature Name	Releases	Feature Information
IP SLAs VoIP Gatekeeper Delay Monitoring	12.3(14)T	The Cisco IOS IP SLAs Voice over IP (VoIP) gatekeeper registration delay operation allows you to measure the average, median, or aggregated network response time of registration attempts from a VoIP gateway to a VoIP gatekeeper device.

Glossary

Gatekeepers --Network devices that help to facilitate and control H.323-based voice and video communications across networks. Gatekeepers are responsible for providing address translation between LAN aliases and IP addresses, call control and routing services to H.323 endpoints, system management, and security policies. These services provided by the gatekeeper in communicating between H.323 endpoints are defined in RAS.

Gateways --Network devices that provide translation between circuit-switched networks (particularly, H.320 ISDN) and packet-based networks (for example, H.323 LANs), allowing endpoints in networks with different transmission formats, codecs, and protocols to communicate.

H.225.0 --Protocol standard that defines the establishment and disconnection of H.323 calls.

H.225.0 RAS --H.225.0 Registration/Admission/Status. Standard that facilitates communication between H.323 gateways (endpoints) and H.323 gatekeepers.

H.235 --Protocol standard that defines security solutions for H.323 protocols (Q.931, H.245, RAS, Streams). H.235 was formerly called H.SECURE.

H.245 --Protocol standard that defines connection management and negotiation capabilities between H.323 devices on the network once the call is established by Q.931.

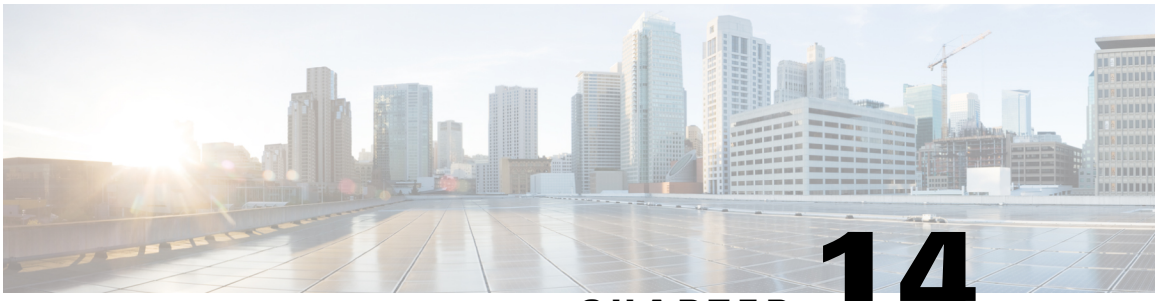
H.323 --An ITU protocol standard for the transmission of real-time audio (Voice/VoIP), video (for example, videoconferencing), and data information over packet switching-based networks. Such networks include IP-based (including the Internet) networks, Internet packet exchange-based local-area networks (LANs), enterprise networks and metropolitan and wide-area networks (WANs). H.323 can also be applied to multipoint

multimedia communications. H.323 defines a distributed architecture for IP telephony applications, including multimedia, video conferencing, video over the Internet, and VoIP.

Q.931 --Protocol standard that defines the establishment and disconnection of H.323 calls.

RTP/RTCP --Real-time Protocol/Real-Time Control Protocol serves as the standardized means for transmitting and receiving audio and video streams across the network once the call is established.

VoIP --Voice or Video over Internet Protocol. Sometimes used to refer to all IP telephony applications.



CHAPTER 14

Configuring VoIP Call Setup Monitoring

The Cisco IOS IP Service Level Agreements (SLAs) VoIP Call Setup (Post-Dial Delay) Monitoring feature provides the ability to measure your network's response time for setting up a Voice over IP (VoIP) call over either H.323 or Session Initiation Protocol (SIP).

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.

Prerequisites for VoIP Call Setup Monitoring

- The Cisco IOS software image on the source and destination gateway must support the IP SLAs VoIP test-call and IP SLAs VoIP Responder applications. To determine if your Cisco IOS software image is configured with these applications, use the **show call application voice**command in EXEC mode.

```
Router# show call application voice summary
NAME            DESCRIPTION
...
```

```
ipsla-testcall   Basic app to place a simple call
ipsla-responder  Basic app to respond to a simple call
...
TCL Script Version 2.0 supported.
Call Treatment Action Application - Version 1.
```

Note The IP SLAs VoIP Responder application is different from the IP SLAs Responder, which is configured using a Cisco IOS command.

Information About VoIP Call Setup Monitoring

IP SLAs VoIP Call Setup Monitoring Using H.323 or SIP

The Cisco IOS IP SLAs VoIP Call Setup Monitoring feature provides the ability to measure your network's response time for setting up a VoIP call. Prior to configuring an IP SLAs VoIP call setup operation, you must enable the IP SLAs VoIP test-call application on the originating gateway (source). With the IP SLAs VoIP test-call application enabled, H.323 or Session Initiation Protocol (SIP) call messages can be sent to and received by the originating (source) and terminating (destination) gateways. The configuration for the IP SLAs VoIP call setup operation is essentially the same for both protocols.

The IP SLAs VoIP call setup operation can measure the total time from when an source gateway sends a call message, containing a call number, to when the sourcegateway receives a response from the destination gateway indicating that either the called number rang or the called party answered the call. As with all Cisco IOS IP SLAs operations, you can configure the VoIP call setup operation to repeat at specified time intervals, for a specified number of repetitions, and over a specified duration of time.

If a gatekeeper (GK) or directory gatekeeper (DGK) is involved in the H.323 call signaling, additional messages are sent and received between the source and destination gateways before the call message is actually sent. The additional time required for these messages is included in the IP SLAs VoIP call setup response time measurement. Likewise, if a proxy server or redirection server is involved in the SIP call signaling, any additional time required for messages to be sent and received prior to sending the call message, is included in the VoIP call setup response time measurement.

A plain old telephone service (POTS) IP phone can be set up at the terminating gateway to respond to an IP SLAs VoIP call setup test call. As an alternative to an actual IP phone, you can enable the IP SLAs VoIP Responder application in the destination gateway. The IP SLAs VoIP Responder application will respond to incoming call setup messages from the source gateway using H.323 or SIP.

How to Configure VoIP Call Setup Monitoring

Configuring the Source Gateway

Note The required configuration for setting up the dial peer will vary slightly depending on whether you are using H.323 or SIP.

SUMMARY STEPS

1. **enable**
2. **call application session start** *instance-name* [*application-name*]
3. **configure terminal**
4. **dial-peer voice** *tag* **voip**
5. **destination-pattern** [+] *string* [**T**]
6. **session target** {**ipv4:** *destination-address* | **dns:**[**s.** | **d.** | **e.** | **u.**] *host-name* | **enum:** *table-num* | **loopback:rtp** | **ras** | **sip-server**}
7. **session protocol sipv2**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**call application session start** *instance-name* [*application-name*] **Example:** `Router# call application session start ipsla-testcall ipsla-testcall`	Starts a new session of the Cisco IOS IP SLAs VoIP test-call application.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 6789 voip`	Defines a VoIP dial peer and enters dial-peer configuration mode.
Step 5	**destination-pattern** [+] *string* [**T**] **Example:** `Router(config-dial-peer)# destination-pattern 6789`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
Step 6	**session target** {**ipv4:** *destination-address* | **dns:**[**s.** | **d.** | **e.** | **u.**] *host-name* | **enum:** *table-num* | **loopback:rtp** | **ras** | **sip-server**}	Designates a network-specific address to receive calls from the VoIP dial peer.

	Command or Action	Purpose
	Example: `Router(config-dial-peer)# session target ipv4:172.29.129.123`	
Step 7	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	(Optional) Specifies SIP as the session protocol for the VoIP dial peer. **Note** Perform this step only if configuring a SIP call.
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode and returns to global configuration mode.

Configuring a VoIP Call Setup Montioring Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **voip delay post-dial** [**detect-point** {**alert-ringing** | **connect-ok**}] **destination** *tag*
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**voip delay post-dial** [**detect-point** {**alert-ringing** | **connect-ok**}] **destination** *tag* **Example:** `Router(config-ip-sla)# voip delay post-dial detect-point alert-ringing destination 6789`	Enters IP SLA VoIP configuration mode and configures the operation as a VoIP call setup (post-dial delay) operation that will generate VoIP call setup response time measurements.
Step 5	**history buckets-kept** *size* **Example:** `Router(config-ip-sla-voip)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-ip-sla-voip)# 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:** `Router(config-ip-sla-voip)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.

	Command or Action	Purpose
Step 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-ip-sla-voip)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	**frequency** *seconds* **Example:** `Router(config-ip-sla-voip)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-ip-sla-voip)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	**history lives-kept** *lives* **Example:** `Router(config-ip-sla-voip)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	**owner** *owner-id* **Example:** `Router(config-ip-sla-voip)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-ip-sla-voip)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	**tag** *text* **Example:** `Router(config-ip-sla-voip)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	**threshold** *milliseconds* **Example:** `Router(config-ip-sla-voip)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 16	**timeout** *milliseconds* **Example:** `Router(config-ip-sla-voip)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	**end** **Example:** `Router(config-ip-sla-voip)# exit`	Exits to privileged EXEC mode.

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*]}]
	
	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.

	Command or Action	Purpose
Step 6	**show ip sla configuration** **Example:** `Device# show ip sla configuration`	(Optional) Displays IP SLAs configuration details.

Enabling the IP SLAs VoIP Responder Application on the Destination Gateway

Note The required configuration for setting up the dial peer will vary slightly depending on whether you are using H.323 or SIP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **incoming called-number** *tag*
5. **application** *application-name*
6. **session protocol sipv2**
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 6789 voip`	Defines a VoIP dial peer and enters dial-peer configuration mode.
Step 4	**incoming called-number** *tag* **Example:** `Router(config-dial-peer)# incoming called-number 6789`	Specifies a digit string to be matched by an incoming call to associate the call with a dial peer.
Step 5	**application** *application-name* **Example:** `Router(config-dial-peer)# application ipsla-responder`	Enables the Cisco IOS IP SLAs VoIP Responder application (ipsla-responder) on the dial peer to respond to incoming call setup messages.
Step 6	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	(Optional) Specifies SIP as the session protocol for the VoIP dial peer. **Note** Perform this step only if configuring a SIP call.
Step 7	**end** **Example:** `Router(config-dial-peer)# exit`	Exits to privileged EXEC mode.

Troubleshooting Tips

- If the IP SLAs operation is not running and not 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 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 SLAs operation, see the “Configuring Proactive Threshold Monitoring” section.

operation)

To display and interpret the results of an IP SLAs operation, use the **show ip sla statistics** command. Check the output for fields that correspond to criteria in your service level agreement to determine whether the service metrics are acceptable.

Configuration Examples for VoIP Call Setup Monitoring

Example VoIP Call Setup Configuration on the Source Gateway

The following example shows the configuration on the source (originating) gateway to start the IP SLAs VoIP test-call application, set up the dial peer to route the test call, define the VoIP call setup operation, and schedule the VoIP call setup operation. In this example, test-call messages are generated using the Session Initiation Protocol (SIP).

```
call application session start ipsla-testcall ipsla-testcall
configure terminal
 dial-peer voice 6789 voip
  destination-pattern 6789
  session target ipv4:172.29.129.123
  session protocol sipv2
  exit
 ip sla 1
  voip delay post-dial detect-point alert-ringing destination 6789
  exit
 ip sla schedule 1 start-time now life forever
```

Example VoIP Responder Application on Destination Gateway

The following example shows the configuration for setting up the dial peer and enabling the IP SLAs VoIP Responder application to respond to the IP SLAs VoIP call setup test call. In this example, test-call messages are generated using the Session Initiation Protocol (SIP).

```
configure terminal
 dial-peer voice 6789 voip
 incoming called-number 6789
 application ipsla-responder
 session protocol sipv2
 exit
```

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*

Related Topic	Document Title
Cisco IOS IP SLAs: general information	Cisco IOS IP SLAs Overview chapter of the *Cisco IP SLAs Configuration Guide*.

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
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

RFCs

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

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

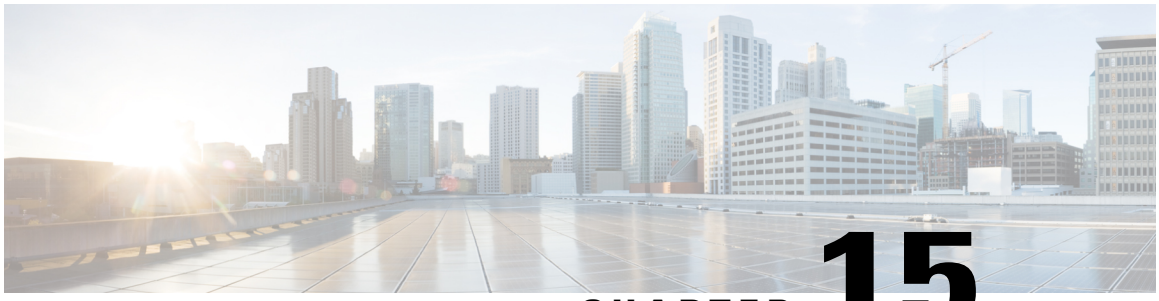
Feature Information for VoIP Call Setup Monitoring

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 28: Feature Information for VoIP Call Setup Monitoring

Feature Name	Releases	Feature Information
IP SLAs VoIP Call Setup (Post Dial Delay) Monitoring	12.3(14)T	The Cisco IOS IP SLAs Voice over IP (VoIP) call setup operation allows you to measure network response time for setting up a VoIP call.



CHAPTER 15

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

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.

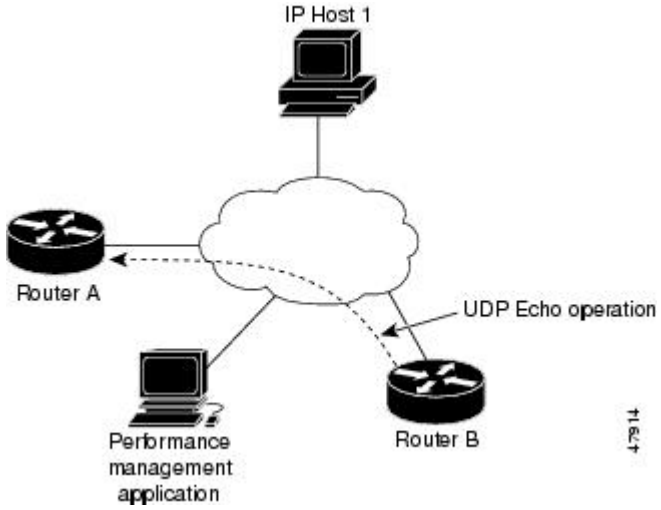
Information About IP SLAs UDP Echo Operations

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 9: 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** *ip-address* **port** *port***vrf** *vrf*	(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:
	`Device(config)# ip sla responder`
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1`
		• Protocol control is enabled by default.

Step 4	**end** **Example:** `Device(config)# end`	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** *operation-number* **Example:** `Device(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*} **source-port** *port-number*] [**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	**data-pattern** *hex value* **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** *seconds* **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 prileged 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** *operation-number* **Example:** `Device(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*} **source-port** *port-number*] [**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** *size* **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** *hex-pattern* **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** *size* **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** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Device(config-ip-sla-udp)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 9	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-udp)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	**frequency** *seconds* **Example:** `Device(config-ip-sla-udp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-udp)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 12	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-udp)# history lives-kept 2`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	**owner** *owner-id* **Example:** `Device(config-ip-sla-udp)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	**request-data-size** *bytes* **Example:** `Device(config-ip-sla-udp)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-udp)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.

	Command or Action	Purpose
Step 16	**tag** *text* **Example:** `Device(config-ip-sla-udp)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-udp)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-udp)# timeout 10000`	(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** *number*
	• **traffic-class** *number*
	Example:
	`Device(config-ip-sla-jitter)# tos 160`
	Example:
	`Device(config-ip-sla-jitter)# traffic-class 160`
		(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** *number* **Example:** `Device(config-ip-sla-udp)# flow-label 112233`	(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:** `Device(config-ip-sla-udp)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	**exit** **Example:** `Device(config-ip-sla-udp)# exit`	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** *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*]}]
	
	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

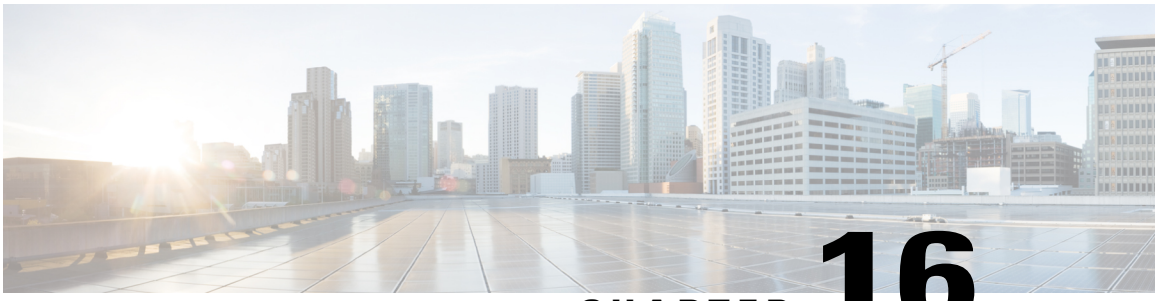
Feature Information for the IP SLAs UDP Echo Operation

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 29: Feature Information for the IP SLAs UDP Echo Operation

Feature Name	Releases	Feature Information
IP SLAs - UDP Echo Operation		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)		Support was added for operability in IPv6 networks.



CHAPTER 16

Configuring IP SLAs HTTP Operations

This module describes how to configure an IP Service Level Agreements (SLAs) HTTP operation to monitor the response time between a Cisco device and an HTTP server to retrieve a web page. The IP SLAs HTTP operation supports both the normal GET requests and customer RAW requests. This module also demonstrates how the results of the HTTP operation can be displayed and analyzed to determine how an HTTP server is performing.

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 HTTP Operations

- IP SLAs HTTP operations support only HTTP/1.0.
- HTTP/1.1 is not supported for any IP SLAs HTTP operation, including HTTP RAW requests.

Information About IP SLAs HTTP Operations

HTTP Operation

The HTTP operation measures the round-trip time (RTT) between a Cisco device and an HTTP server to retrieve a web page. The HTTP server response time measurements consist of three types:

- DNS lookupRTT taken to perform domain name lookup.
- TCP Connect--RTT taken to perform a TCP connection to the HTTP server.
- HTTP transaction time--RTT taken to send a request and get a response from the HTTP server. The operation retrieves only the home HTML page.

The DNS operation is performed first and the DNS RTT is measured. Once the domain name is found, a TCP Connect operation to the appropriate HTTP server is performed and the RTT for this operation is measured. The final operation is an HTTP request and the RTT to retrieve the home HTML page from the HTTP server is measured. One other measurement is made and called the time to first byte which measures the time from the start of the TCP Connect operation to the first HTML byte retrieved by the HTTP operation. The total HTTP RTT is a sum of the DNS RTT, the TCP Connect RTT, and the HTTP RTT.

For GET requests, IP SLAs will format the request based on the specified URL. For RAW requests, IP SLAs requires the entire content of the HTTP request. When a RAW request is configured, the raw commands are specified in HTTP RAW configuration mode. A RAW request is flexible and allows you to control fields such as authentication. An HTTP request can be made through a proxy server.

The results of an HTTP operation can be useful in monitoring your web server performance levels by determining the RTT taken to retrieve a web page.

Regardless of the HTTP errors, the IP SLA works fine. Currently, the error codes are determined, and the IP SLA HTTP operation goes down only if the return code is not 200.

Note The only time the SLA probe goes down is when the SLA is unable to establish a TCP connection or is unable to receive an answer from the Remote server to its HTTP request.

How to Configure IP SLAs HTTP Operations

Configuring an HTTP GET Operation on the Source Device

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

Perform only one of the following tasks:

Configuring a Basic HTTP GET Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]
5. **frequency** *seconds*
6. **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	**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	**http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*] **Example:** `Device(config-ip-sla)# http get http://198.133.219.25`	Defines an HTTP operation and enters IP SLA configuration mode.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-http)# frequency 90`	(Optional) Sets the rate at which a specified IP SLAs HTTP operation repeats. The default and minimum frequency value for an IP SLAs HTTP operation is 60 seconds.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-ip-sla-http)# end`	Exits to privileged EXEC mode.

Configuring an HTTP GET Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]
5. **history distributions-of-statistics-kept** *size*
6. **frequency** *seconds*
7. **history hours-of-statistics-kept** *hours*
8. **http-raw-request**
9. **owner** *owner-id*
10. **history statistics-distribution-interval** *milliseconds*
11. **tag** *text*
12. **threshold** *milliseconds*
13. **timeout** *milliseconds*
14. **tos** *number*
15. **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.

	Command or Action	Purpose
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	**http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*] **Example:** `Device(config-ip-sla)# http get http://198.133.219.25`	Defines an HTTP operation and enters IP SLA configuration mode.
Step 5	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-http)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 6	**frequency** *seconds* **Example:** `Device(config-ip-sla-http)# frequency 90`	(Optional) Sets the rate at which a specified IP SLAs HTTP operation repeats. The default and minimum frequency value for an IP SLAs HTTP operation is 60 seconds.
Step 7	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-http)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 8	**http-raw-request** **Example:** `Device(config-ip-sla-http)# http-raw-request`	(Optional) Explicitly specifies the options for a GET request for an IP SLAs HTTP operation.
Step 9	**owner** *owner-id* **Example:** `Device(config-ip-sla-http)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 10	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-http)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 11	**tag** *text* **Example:** `Device(config-ip-sla-http)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 12	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-http)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 13	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-http)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 14	**tos** *number* **Example:** `Device(config-ip-sla-http)# tos 160`	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 15	**end** **Example:** `Device(config-ip-sla-http)# end`	Exits to privileged EXEC mode.

Configuring an HTTP RAW Operation on the Source Device

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. **http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]
5. **http-raw-request**
6. Enter the required HTTP 1.0 command syntax.
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** *operation-number* **Example:** `Device(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**http** {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*] **Example:** `Device(config-ip-sla)# http raw http://198.133.219.25`	Defines an HTTP operation.
Step 5	**http-raw-request** **Example:** `Device(config-ip-sla)# http-raw-request`	Enters HTTP RAW configuration mode.
Step 6	Enter the required HTTP 1.0 command syntax. **Example:** `Device(config-ip-sla-http)# GET /en/US/hmpgs/index.html HTTP/1.0\r\n\r\n`	Specifies all the required HTTP 1.0 commands.
Step 7	**end** **Example:** `Device(config-ip-sla-http)# end`	Exits to privileged EXEC mode.

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**]	• 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

	• **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*]}]
	
	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`	

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

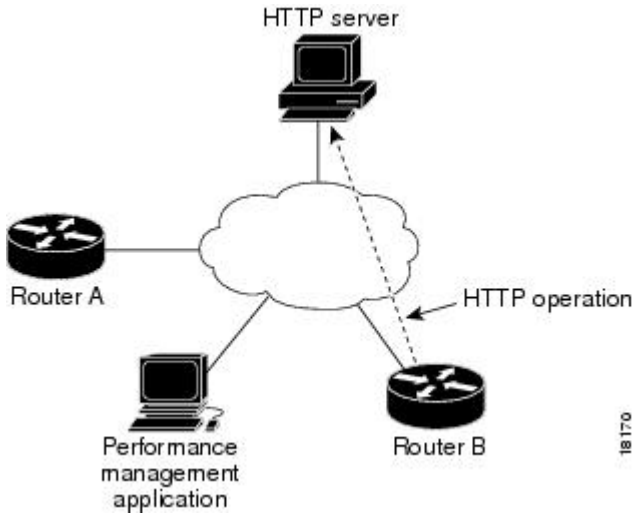
To add proactive threshold conditions and reactive triggering for generating traps (or for starting another operation) to an IP Service Level Agreements (SLAs) operation, see the "Configuring Proactive Threshold Monitoring" section.

Configuration Examples for IP SLAs HTTP Operations

Example Configuring an HTTP GET Operation

The following example show how to create and configure operation number 8 as an HTTP GET operation. The destination URL IP address represents the www.cisco.com website. The following figure depicts the HTTP GET operation.

Figure 10: HTTP Operation



Device B Configuration

```
ip sla 8
 http get url http://198.133.219.25
!
ip sla schedule 8 start-time now
```

Example Configuring an HTTP RAW Operation

The following example shows how to configure an HTTP RAW operation. To use the RAW commands, enter HTTP RAW configuration mode by using the **http-raw-request** command in IP SLA configuration mode. The IP SLA HTTP RAW configuration mode is indicated by the (config-ip-sla-http) router prompt.

```
ip sla 8
 http raw url http://198.133.219.25
 http-raw-request
 GET /en/US/hmpgs/index.html HTTP/1.0\r\n
 \r\n
 end
ip sla schedule 8 life forever start-time now
```

Example Configuring an HTTP RAW Operation Through a Proxy Server

The following example shows how to configure an HTTP RAW operation through a proxy server. The proxy server is www.proxy.cisco.com and the HTTP server is www.yahoo.com.

```
ip sla 8
 http raw url http://www.proxy.cisco.com
 http-raw-request
 GET http://www.yahoo.com HTTP/1.0\r\n
 \r\n
 end
ip sla schedule 8 life forever start-time now
```

Example Configuring an HTTP RAW Operation with Authentication

The following example shows how to configure an HTTP RAW operation with authentication.

```
ip sla 8
 http raw url http://site-test.cisco.com
 http-raw-request
 GET /lab/index.html HTTP/1.0\r\n
 Authorization: Basic btNpdGT4biNvoZe=\r\n
 \r\n
 end
ip sla schedule 8 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
No new or modified standards or RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

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

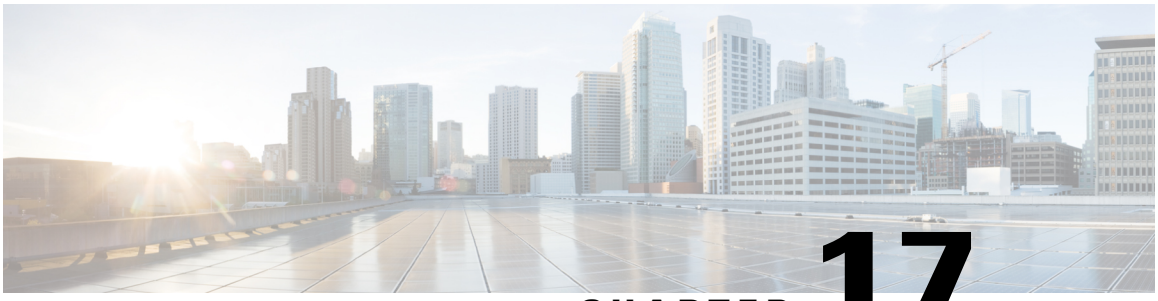
Feature Information for IP SLAs HTTP Operations

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 30: Feature Information for IP SLAs HTTP Operations

Feature Name	Releases	Feature Information
IP SLAs HTTP Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs Hypertext Transfer Protocol (HTTP) operation allows you to measure the network response time between a Cisco device and an HTTP server to retrieve a web page.
IPSLA 4.0 - IP v6 phase2	15.2(3)T 15.1(2)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: **http (IP SLA)**, **show ip sla configuration**, **show ip sla summary**.
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY	Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 17

Configuring IP SLAs TCP Connect Operations

This module describes how to configure an IP Service Level Agreements (SLAs) TCP Connect operation to measure the response time taken to perform a TCP Connect operation between a Cisco router and devices using IPv4 or IPv6. TCP Connect accuracy is enhanced by using the IP SLAs Responder at the destination Cisco router. This module also demonstrates how the results of the TCP Connect operation can be displayed and analyzed to determine how the connection times to servers and hosts within your network can affect IP service levels. The TCP Connect operation is useful for measuring response times for a server used for a particular application or connectivity testing for server availability.

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.

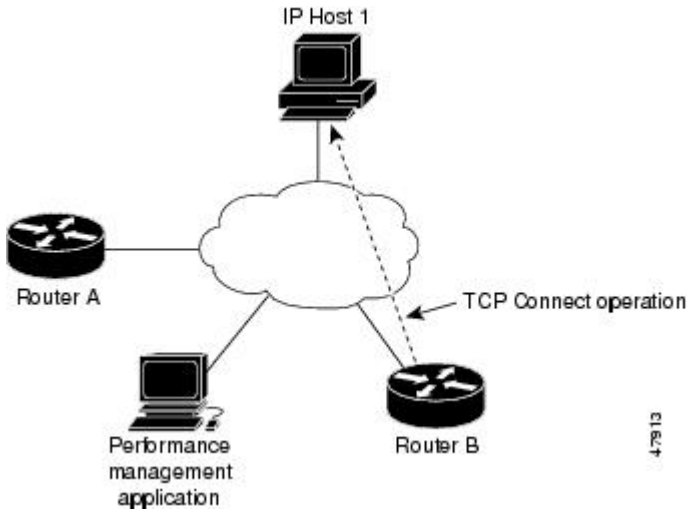
Information About the IP SLAs TCP Connect Operation

TCP Connect Operation

The IP SLAs TCP Connect operation measures the response time taken to perform a TCP Connect operation between a Cisco device and devices using IP. TCP is a transport layer (Layer 4) Internet protocol that provides reliable full-duplex data transmission. The destination device can be any device using IP or an IP SLAs Responder.

In the figure below Device B is configured as the source IP SLAs device and a TCP Connect operation is configured with the destination device as IP Host 1.

Figure 11: TCP Connect Operation



Connection response time is computed by measuring the time taken between sending a TCP request message from Device B to IP Host 1 and receiving a reply from IP Host 1.

TCP Connect accuracy is enhanced by using the IP SLAs Responder at the destination Cisco device. If the destination device is a Cisco device, then IP SLAs makes a TCP connection to any port number that you specified. If the destination is not a Cisco IP host, then you must specify a known destination port number such as 21 for FTP, 23 for Telnet, or 80 for an HTTP server.

Using the IP SLAs Responder is optional for a TCP Connect operation when using Cisco devices. The IP SLAs Responder cannot be configured on non-Cisco devices.

TCP Connect is used to test virtual circuit availability or application availability. Server and application connection performance can be tested by simulating Telnet, SQL, and other types of connection to help you verify your IP service levels.

How to Configure the IP SLAs TCP Connect Operation

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. Do one of the following:
   - **ip sla responder**
   - **ip sla responder tcp-connect ipaddress** *ip-address* **port** *port*
4. **exit**

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	Do one of the following: • **ip sla responder** • **ip sla responder tcp-connect ipaddress** *ip-address* **port** *port* **Example:** `Device(config)# ip sla responder`	(Optional) Temporarily enables IP SLAs responder functionality on the Cisco device in response to control messages from source. or (Optional) Required only if protocol control is explicitly disabled on the source device. Permanently enables IP SLAs responder functionality on the specified IP address and port. • Control is enabled by default.

	Command or Action	Purpose
	Example: `Device(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000`	
Step 4	**exit** **Example:** `Device(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a TCP Connect Operation on the Source Device

Perform only one of the following tasks:

Prerequisites

If you are using the IP SLAs Responder, complete the "Configuring the IP SLAs Responder on the Destination Device" section before you start this task.

Configuring a Basic TCP Connect Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **frequency** *seconds*
6. **end**

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	**tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}] **Example:** `Device(config-ip-sla)# tcp-connect 172.29.139.132 5000`	Defines a TCP Connect operation and enters IP SLA TCP 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	**frequency** *seconds* **Example:** `Device(config-ip-sla-tcp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**end** **Example:** `Device(config-ip-sla-tcp)# end`	Returns to global configuration mode.

Troubleshooting Tips

- If the IP SLAs operation is not running and not 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 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 SLAs operation, see the "Configuring Proactive Threshold Monitoring" section.

operation)

To display and interpret the results of an IP SLAs operation, use the **show ip sla statistics** command. Check the output for fields that correspond to criteria in your service level agreement to determine whether the service metrics are acceptable.

Configuring a TCP Connect Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **tcp-connect** {*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. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. Do one of the following:
    - **tos** *number*
    - **traffic-class** *number*
18. **flow-label** *number*
19. **exit**
20. **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`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}] **Example:** `Device(config-ip-sla)# tcp-connect 172.29.139.132 5000`	Defines a TCP Connect operation and enters IP SLA TCP 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** *size* **Example:** `Device(config-ip-sla-tcp)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-tcp)# 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:** `Device(config-ip-sla-tcp)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-tcp)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.

	Command or Action	Purpose
Step 9	**frequency** *seconds* **Example:** `Device(config-ip-sla-tcp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-tcp)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-tcp)# history lives-kept 2`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	**owner** *owner-id* **Example:** `Device(config-ip-sla-tcp)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-tcp)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	**tag** *text* **Example:** `Device(config-ip-sla-tcp)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-tcp)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-tcp)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	Do one of the following: • **tos** *number* • **traffic-class** *number*	(Optional) For IPv4: Defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) For IPv6: 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`
	
	Example:
	`Device(config-ip-sla-jitter)# traffic-class 160`	

Step 18	**flow-label** *number* **Example:** `Device(config-ip-sla-tcp)# flow-label 112233`	(Optional) For IPv6: Defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 19	**exit** **Example:** `Device(config-ip-sla-tcp)# exit`	Exits TCP configuration submode and returns to global configuration mode.
Step 20	**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.

Troubleshooting Tips

- If the IP SLAs operation is not running and not 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 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 SLAs operation, see the “Configuring Proactive Threshold Monitoring” section.

operation)

To display and interpret the results of an IP SLAs operation, use the **show ip sla statistics** command. Check the output for fields that correspond to criteria in your service level agreement to determine whether the service metrics are acceptable.

Configuration Examples for IP SLAs TCP Connect Operations

Example Configuring a TCP Connect Operation

The following example shows how to configure a TCP Connect operation from Device B to the Telnet port (TCP port 23) of IP Host 1 (IP address 10.0.0.1), as shown in the "TCP Connect Operation" figure in the "Information About the IP SLAs TCP Connect Operation" section. The operation is scheduled to start immediately. In this example, the control protocol is disabled on the source (Device B). IP SLAs uses the control protocol to notify the IP SLAs responder to enable the target port temporarily. This action allows the responder to reply to the TCP Connect operation. In this example, because the target is not a Cisco device and a well-known TCP port is used, there is no need to send the control message.

Device A (target device) Configuration

```
configure terminal
 ip sla responder tcp-connect ipaddress 10.0.0.1 port 23
```

Device B (source device) Configuration

```
ip sla 9
 tcp-connect 10.0.0.1 23 control disable
 frequency 30
 tos 128
 timeout 1000
 tag FLL-RO
ip sla schedule 9 start-time now
```

The following example shows how to configure a TCP Connect operation with a specific port, port 23, and without an IP SLAs responder. The operation is scheduled to start immediately and run indefinitely.

```
ip sla 9
 tcp-connect 173.29.139.132 21 control disable
 frequency 30
ip sla schedule 9 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

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

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

RFCs

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

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

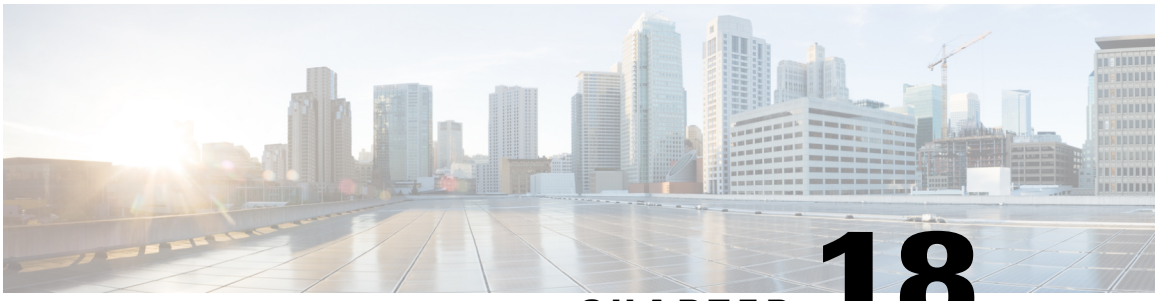
Feature Information for the IP SLAs TCP Connect Operation

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 31: Feature Information for the IP SLAs TCP Connect Operation

Feature Name	Releases	Feature Information
IP SLAs TCP Connect Operation		The Cisco IOS IP SLAs Transmission Control Protocol (TCP) connect operation allows you to measure the network response time taken to perform a TCP Connect operation between a Cisco device and other devices using IP.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)		Support was added for operability in IPv6 networks.
IP SLAs VRF Aware 2.0		Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 18

Configuring IP SLAs ICMP Echo Operations

This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. ICMP Echo is useful for troubleshooting network connectivity issues. This module also demonstrates how the results of the ICMP Echo operation can be displayed and analyzed to determine how the network IP connections are performing.

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 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.

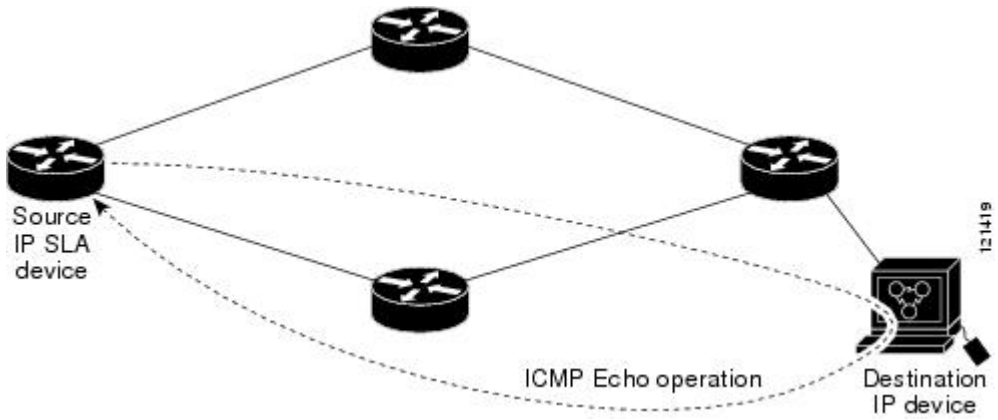
Information About IP SLAs ICMP Echo Operations

ICMP Echo Operation

The ICMP Echo operation measures end-to-end response time between a Cisco router and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP Echo request message to the destination and receiving an ICMP Echo reply.

In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements.

Figure 12: ICMP Echo Operation



The IP SLAs ICMP Echo operation conforms to the same IETF specifications for ICMP ping testing and the two methods result in the same response times.

How to Configure IP SLAs ICMP Echo Operations

Configuring an ICMP Echo Operation

Note There is no need to configure an IP SLAs responder on the destination device.

Perform one of the following tasks:

Configuring a Basic ICMP Echo Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]
5. **frequency** *seconds*
6. **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	**ip sla** *operation-number* **Example:** `Device(config)# ip sla 6`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*] **Example:** `Device(config-ip-sla)# icmp-echo 172.29.139.134`	Defines an ICMP Echo operation and enters IP SLA ICMP Echo configuration mode.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-echo)# frequency 300`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-ip-sla-echo)# end`	Exits 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 an ICMP Echo Operation with Optional Parameters

Perform this task on the source device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]
5. **data-pattern** *hex value*
6. **history buckets-kept** *size*
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. **vrf** *vrf-name*
23. **end**

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 6`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*] **Example:** `Device(config-ip-sla)# icmp-echo 172.29.139.134 source-ip 172.29.139.132`	Defines an Echo operation and enters IP SLA Echo configuration mode.
Step 5	**data-pattern** *hex value* **Example:** `Device(config-ip-sla-echo)# data pattern FFFFFFFF`	(Optional) Sets the hexadecimal value for data pattern. The range is 0 to FFFFFFFF.
Step 6	**history buckets-kept** *size* **Example:** `Device(config-ip-sla-echo)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 7	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-echo)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 8	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Device(config-ip-sla-echo)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.

	Command or Action	Purpose
Step 9	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-echo)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	**frequency** *seconds* **Example:** `Device(config-ip-sla-echo)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-echo)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 12	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-echo)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	**owner** *owner-id* **Example:** `Device(config-ip-sla-echo)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	**request-data-size** *bytes* **Example:** `Device(config-ip-sla-echo)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-echo)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	**tag** *text* **Example:** `Device(config-ip-sla-echo)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 17	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-echo)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-echo)# timeout 10000`	(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** *number*
	• **traffic-class** *number*
	Example:
	`Device(config-ip-sla-jitter)# tos 160`
	Example:
	`Device(config-ip-sla-jitter)# traffic-class 160`
		(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** *number* **Example:** `Device(config-ip-sla-echo)# flow-label 112233`	(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:** `Device(config-ip-sla-echo)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-echo)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 23	**end** **Example:** `Device(config-ip-sla-echo)# end`	Exits 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.

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.

	Command or Action	Purpose

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*]}]
	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 ICMP Echo Operations

Example Configuring an ICMP Echo Operation

The following example shows how to configure an IP SLAs operation type of ICMP Echo that will start immediately and run indefinitely.

```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
 request-data-size 28
 tos 160
 timeout 2000
 tag SFO-RO
ip sla schedule 6 life forever start-time now
```

Additional References for IP SLAs ICMP Echo Operations

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP SLAs commands	Cisco IOS IP SLAs Command Reference
Information about Cisco IP SLAs	"Cisco IOS IP SLAs Overview" module of the *IP SLAs Configuration Guide*

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

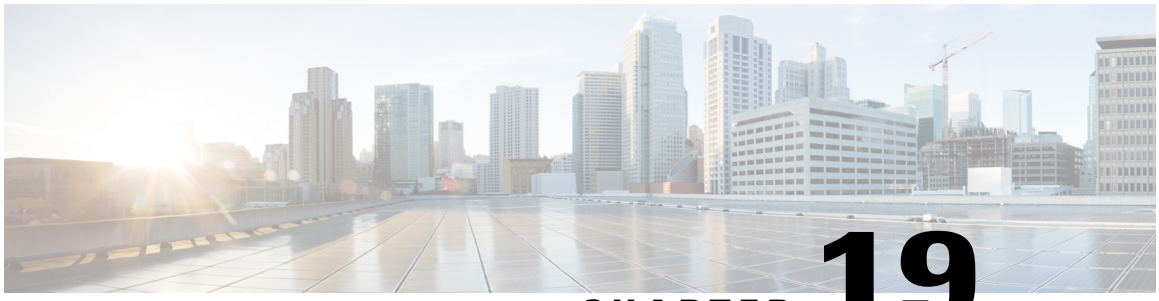
Feature Information for IP SLAs ICMP Echo Operations

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 32: Feature Information for IP SLAs ICMP Echo Operations

Feature Name	Releases	Feature Information
IP SLAs ICMP Echo Operation		The Cisco IOS IP SLAs Internet Control Message Protocol (ICMP) echo operation allows you to measure end-to-end network response time between a Cisco device and other devices using IP.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)		Support was added for operability in IPv6 networks.



CHAPTER 19

Configuring IP SLAs ICMP Path Echo Operations

This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Path Echo operation to monitor end-to-end and hop-by-hop response time between a Cisco device and other devices using IP. ICMP Path Echo is useful for determining network availability and for troubleshooting network connectivity issues. The results of the ICMP Path Echo operation can be displayed and analyzed to determine how ICMP is performing.

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 Path 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 ICMP Path Echo Operations

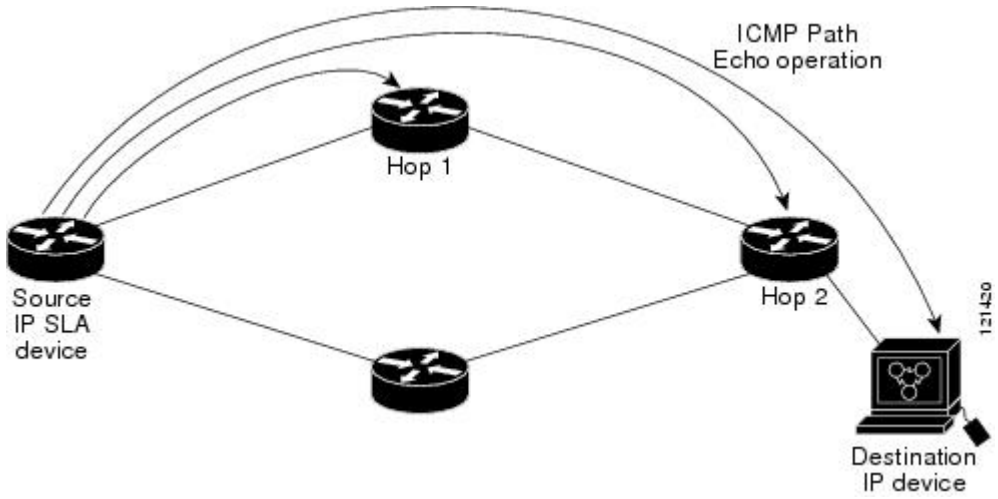
ICMP Path Echo Operation

To monitor ICMP Path Echo performance on a device, use the IP SLAs ICMP Path Echo operation. An ICMP Path Echo operation measures end-to-end and hop-by-hop response time between a Cisco device and other devices using IP. ICMP Path Echo is useful for determining network availability and for troubleshooting network connectivity issues.

The IP SLAs ICMP Path Echo operation records statistics for each hop along the path that the IP SLAs operation takes to reach its destination. The ICMP Path Echo operation determines this hop-by-hop response time between a Cisco device and any IP device on the network by discovering the path using the traceroute facility.

In the figure below the source IP SLAs device uses traceroute to discover the path to the destination IP device. A ping is then used to measure the response time between the source IP SLAs device and each subsequent hop in the path to the destination IP device.

Figure 13: ICMP Path Echo Operation



Using the statistics recorded for the response times and availability, the ICMP Path Echo operation can identify a hop in the path that is causing a bottleneck.

How to Configure IP SLAs ICMP Path Echo Operations

Configuring an ICMP Path Echo Operation on the Source Device

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

Perform only one of the following tasks:

Configuring a Basic ICMP Path Echo Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-id*
4. **path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **frequency** *seconds*
6. **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	**ip sla** *operation-id* **Example:** `Device(config)# ip sla 7`	Specifies an ID number for the operation being configured, and enters IP SLA configuration mode.
Step 4	**path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.

	Command or Action	Purpose
	Example: `Device(config-ip-sla)# path-echo 172.29.139.134`	
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-pathEcho)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**end** **Example:** `Device(config-ip-sla-pathEcho)# end`	Exits to privileged EXEC mode.

Example

The following example shows the configuration of the IP SLAs ICMP Path Echo operation number 7 that will start in 30 seconds and run for 5 minutes.

```
ip sla 7
 path-echo 172.29.139.134
 frequency 30
!
ip sla schedule 7 start-time after 00:00:30 life 300
```

Configuring an ICMP Path Echo Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history filter** {**none** | **all** | **overThreshold** | **failures**}
8. **frequency** *seconds*
9. **history hours-of-statistics-kept** *hours*
10. **history lives-kept** *lives*
11. **owner** *owner-id*
12. **paths-of-statistics-kept** *size*
13. **request-data-size** *bytes*
14. **samples-of-history-kept** *samples*
15. **history statistics-distribution-interval** *milliseconds*
16. **tag** *text*
17. **threshold** *milliseconds*
18. **timeout** *milliseconds*
19. **tos** *number*
20. **verify-data**
21. **vrf** *vrf-name*
22. **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.

	Command or Action	Purpose
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	**path-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] **Example:** `Device(config-ip-sla)# path-echo 172.29.139.134`	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.
Step 5	**history buckets-kept** *size* **Example:** `Device(config-ip-sla-pathEcho)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-pathEcho)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-pathEcho)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 8	**frequency** *seconds* **Example:** `Device(config-ip-sla-pathEcho)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 9	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-pathEcho)# 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 10	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-pathEcho)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 11	**owner** *owner-id* **Example:** `Device(config-ip-sla-pathEcho)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 12	**paths-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-pathEcho)# paths-of-statistics-kept 3`	(Optional) Sets the number of paths for which statistics are maintained per hour for an IP SLAs operation.
Step 13	**request-data-size** *bytes* **Example:** `Device(config-ip-sla-pathEcho)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 14	**samples-of-history-kept** *samples* **Example:** `Device(config-ip-sla-pathEcho)# samples-of-history-kept 10`	(Optional) Sets the number of entries kept in the history table per bucket for an IP SLAs operation.
Step 15	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-pathEcho)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	**tag** *text* **Example:** `Device(config-ip-sla-pathEcho)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-pathEcho)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 18	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-pathEcho)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	**tos** *number* **Example:** `Device(config-ip-sla-pathEcho)# tos 160`	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 20	**verify-data** **Example:** `Device(config-ip-sla-pathEcho)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 21	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-pathEcho)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 22	**end** **Example:** `Device(config-ip-sla-pathEcho)# end`	Exits to privileged EXEC mode.

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 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`	

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

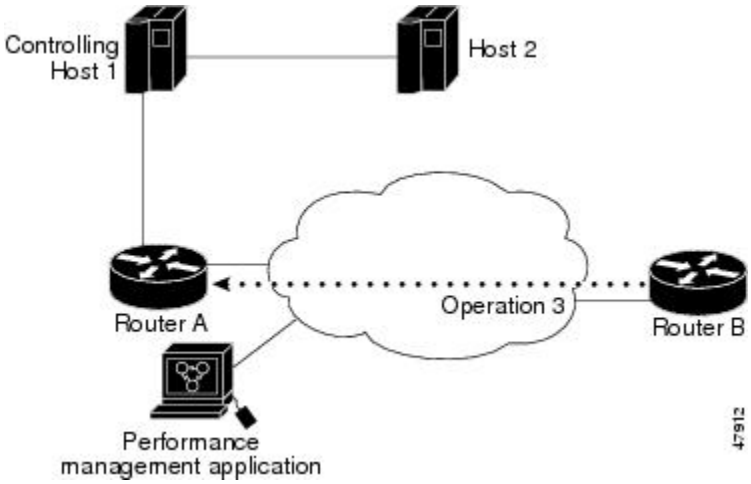
To add proactive threshold conditions and reactive triggering for generating traps (or for starting another operation) to an IP Service Level Agreements (SLAs) operation, see the "Configuring Proactive Threshold Monitoring" section.

Configuration Examples for IP SLAs ICMP Path Echo Operations

Example Configuring an ICMP Path Echo Operation

The following example shows how to configure an IP SLAs operation type of ICMP Path Echo that will start after 30 seconds and run for 5 minutes. The figure below depicts the ICMP Path Echo operation.

Figure 14: ICMP Path Echo Operation



This example sets a Path Echo operation (ip sla 3) from Device B to Device A using IP/ICMP. The operation attempts to execute three times in 25 seconds (first attempt at 0 seconds).

Device B Configuration

```
ip sla 3
 path-echo 172.29.139.134
 frequency 10
 tag SGN-RO
 timeout 1000
ip sla schedule 3 life 25
```

Additional References for IP SLAs ICMP Echo Operations

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP SLAs commands	Cisco IOS IP SLAs Command Reference
Information about Cisco IP SLAs	"Cisco IOS IP SLAs Overview" module of the *IP SLAs Configuration Guide*

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

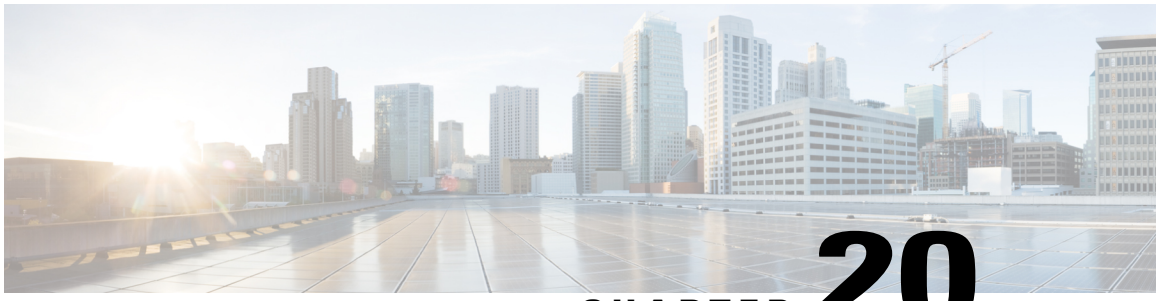
Feature Information for IP SLAs ICMP Path Echo Operations

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 33: Feature Information for IP SLAs ICMP Path Echo Operations

Feature Name	Releases	Feature Information
IP SLAs ICMP Path Echo Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs Internet Control Message Protocol (ICMP) path echo operation allows you to measure end-to-end and hop-by-hop network response time between a Cisco device and other devices using IP.
IP SLA 4.0 - IP v6 phase2	15.2(3)T Cisco IOS XE Release 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: **path-echo** (IP SLA), **show ip sla configuration**, **show ip sla summary**.



CHAPTER 20

Configuring IP SLAs ICMP Path Jitter Operations

This document describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Path Jitter operation to monitor hop-by-hop jitter (inter-packet delay variance). This document also demonstrates how the data gathered using the Path Jitter operations can be displayed and analyzed using Cisco 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.

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 ICMP Path Jitter Operations

- 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.

- In contrast with other IP SLAs operations, the IP SLAs Responder does not have to be enabled on either the target device or intermediate devices for Path Jitter operations. However, the operational efficiency may improve if you enable the IP SLAs Responder.

Restrictions for ICMP Path Jitter Operations

- IP SLAs - ICMP Path Jitter is ICMP-based. ICMP-based operations can compensate for source processing delay but cannot compensate for target processing delay. For more robust monitoring and verifying, we recommend that you use the IP SLAs UDP Jitter operation.
- The jitter values obtained using IP SLAs - ICMP Path Jitter are approximates because ICMP does not provide the capability to embed processing times on devices in the packet. If the target device does not place ICMP packets as the highest priority, then the device will not respond properly. ICMP performance also can be affected by the configuration of priority queueing on the device and by ping response.
- A path jitter operation does not support hourly statistics and hop information.
- Unlike other IP SLAs operations, the ICMP Path Jitter operation is not supported in the RTTMON MIB. Path jitter operations can only be configured using Cisco commands and statistics can only be returned using the **show ip sla** commands.
- IP SLAs - Path Jitter does not support the IP SLAs History feature (statistics history buckets) because of the large data volume involved with jitter operations.
- The following commands, available in path jitter configuration mode, do not apply to path jitter operations:
  - **history buckets-kept**
  - **history distributions-of-statistics-kept**
  - **history enhanced**
  - **history filter**
  - **history hours-of-statistics-kept**
  - **history lives-kept**
  - **history statistics-distribution-interval**
  - **samples-of-history-kept**
  - **lsr-path**
  - **tos**
  - **threshold**
  - **verify-data**

Information About IP SLAs ICMP Path Jitter Operations

ICMP Path Jitter Operation

IP SLAs - ICMP Path Jitter provides hop-by-hop jitter, packet loss, and delay measurement statistics in an IP network. Path jitter operations function differently than the standard UDP Jitter operation, which provides total one-way data and total round-trip data.

An ICMP Path Jitter operation can be used a supplement to the standard UDP Jitter operation. For example, results from a UDP Jitter operation may indicate unexpected delays or high jitter values; an ICMP Path Jitter operation could then be used to troubleshoot the network path and determine if traffic is bottlenecking in a particular segment along the transmission path.

The operation first discovers the hop-by-hop IP route from the source to the destination using a traceroute utility, and then uses ICMP echoes to determine the response times, packet loss and approximate jitter values for each hop along the path. The jitter values obtained using IP SLAs - ICMP Path Jitter are approximates because ICMP only provides round trip times.

ICMP Path Jitter operations function by tracing the IP path from a source device to a specified destination device, then sending *N* number of Echo probes to each hop along the traced path, with a time interval of *T* milliseconds between each Echo probe. The operation as a whole is repeated at a frequency of once every *F* seconds. The attributes are user-configurable, as shown here:

Path Jitter Operation Parameter	Default	Configured Using:
Number of echo probes (*N*)	10 echos	**path-jitter** command, **num-packets** option
Time between Echo probes, in milliseconds (*T*)	20 ms	**path-jitter** command, **interval** option **Note** The operation's frequency is different than the operation's interval.
The frequency of how often the operation is repeated (*F*)	once every 60 seconds	**frequency** command

How to Configure the IP SLAs ICMP Path Jitter Operation

Configuring the IP SLAs Responder on a Destination Device

Note An IP SLAs Responder is not required on either the target device or intermediate devices for path jitter operations. However, operational efficiency may improve if you enable the IP SLAs Responder.

Before You Begin

The networking device to be used as the responder must be a Cisco device and you must have connectivity to that device through the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder**
4. **exit**

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 responder** **Example:** **Example:** `Device(config)# ip sla responder`	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. • Control is enabled by default.
Step 4	**exit** **Example:** `Device(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring an ICMP Path Jitter Operation on the Source Device

Perform only one of the following procedures in this section:

Configuring a Basic ICMP Path Jitter Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**]
5. **frequency** *seconds*
6. **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	**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	**path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**] **Example:** `Device(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22`	Enters IP SLA Path Jitter configuration mode for configuring an ICMP Path Jitter operation.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-pathJitter)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-ip-sla-pathJitter)# end`	Exits to privileged EXEC mode.

Example

In the following example, the **targetOnly** keyword is used to bypass the hop-by-hop measurements. With this version of the command, echo probes will be sent to the destination only.

```
Device(config)# ip sla 1
Device(config-ip-sla)# path-jitter 172.17.246.20 num-packets 50 interval 30 targetOnly
```

Configuring an ICMP Path Jitter Operation with Additional Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**]
5. **frequency** *seconds*
6. **owner** *owner-id*
7. **request-data-size** *bytes*
8. **tag** *text*
9. **timeout** *milliseconds*
10. **vrf** *vrf-name*
11. **end**

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	**path-jitter** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**] **Example:** `Device(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22`	Enters IP SLA Path Jitter configuration mode for defing an ICMP Path Jitter operation.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-pathJitter)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**owner** *owner-id* **Example:** `Device(config-ip-sla-pathJitter)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 7	**request-data-size** *bytes* **Example:** `Device(config-ip-sla-pathJitter)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 8	**tag** *text* **Example:** `Device(config-ip-sla-pathJitter)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 9	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-pathJitter)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 10	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-pathJitter)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 11	**end** **Example:** `Device(config-ip-sla-pathJitter)# end`	Exits to privileged EXEC mode.

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 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`	

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 ICMP Path Jitter Operations

Example Configuring a Path Jitter Operation

The following example shows the output when the ICMP Path Jitter operation is configured. Because the path jitter operation does not support hourly statistics and hop information, the output for the **show ip sla statistics** command for the path jitter operation displays only the statistics for the first hop.

The following example shows the output when the ICMP Path Jitter operation is configured.

```
Device# configure terminal
Device(config)# ip sla 15011
Device(config-sla-monitor)# path-jitter 10.222.1.100 source-ip 10.222.3.100 num-packets 20
Device(config-sla-monitor-pathJitter)# frequency 30
Device(config-sla-monitor-pathJitter)# exit
Device(config)# ip sla schedule 15011 life forever start-time now
Device(config)# exit
Device# show ip sla statistics 15011
Round Trip Time (RTT) for       Index 15011
        Latest RTT: 1 milliseconds
Latest operation start time: 15:37:35.443 EDT Mon Jun 16 2008
Latest operation return code: OK
---- Path Jitter Statistics ----
Hop IP 10.222.3.252:
Round Trip Time milliseconds:
        Latest RTT: 1 ms
        Number of RTT: 20
        RTT Min/Avg/Max: 1/1/3 ms
Jitter time milliseconds:
        Number of jitter: 2
        Jitter Min/Avg/Max: 2/2/2 ms
Packet Values:
        Packet Loss (Timeouts): 0
        Out of Sequence: 0
        Discarded Samples: 0
Operation time to live: Forever
```

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 1889[4]	*RTP: A Transport Protocol for Real-Time Applications* ; see the section "Estimating the Interarrival Jitter"

4 Support for the listed RFC is not claimed; listed as a reference only.

MIBs

MIBs	MIBs Link
MIB support for the Path Jitter operation is not provided.	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

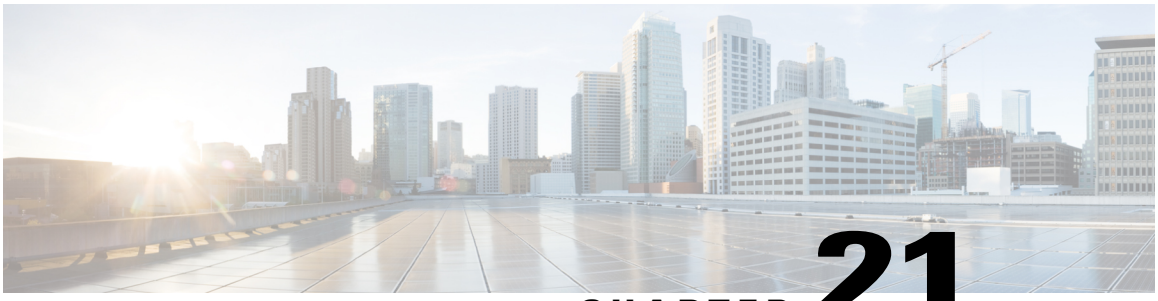
Feature Information for IP SLAs ICMP Path Jitter Operations

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 34: Feature Information for IP SLAs ICMP Path Jitter Operations

Feature Name	Releases	Feature Information
IP SLAs Path Jitter Operation		The Cisco IOS IP SLAs Internet Control Message Protocol (ICMP) path jitter operation allows you to measure hop-by-hop jitter (inter-packet delay variance).
IPSLA 4.0 - IP v6 phase2		Support was added for operability in IPv6 networks. The following commands are introduced or modified: **path-jitter**, **show ip sla configuration**, **show ip sla summary**.



CHAPTER 21

Configuring IP SLAs FTP Operations

This module describes how to configure an IP Service Level Agreements (SLAs) File Transfer Protocol (FTP) operation to measure the response time between a Cisco device and an FTP server to retrieve a file. The IP SLAs FTP operation supports an FTP GET request only. This module also demonstrates how the results of the FTP operation can be displayed and analyzed to determine the capacity of your network. The FTP operation can be used also for troubleshooting FTP server performance.

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 FTP Operations

The IP SLAs FTP operation only supports FTP GET (download) requests.

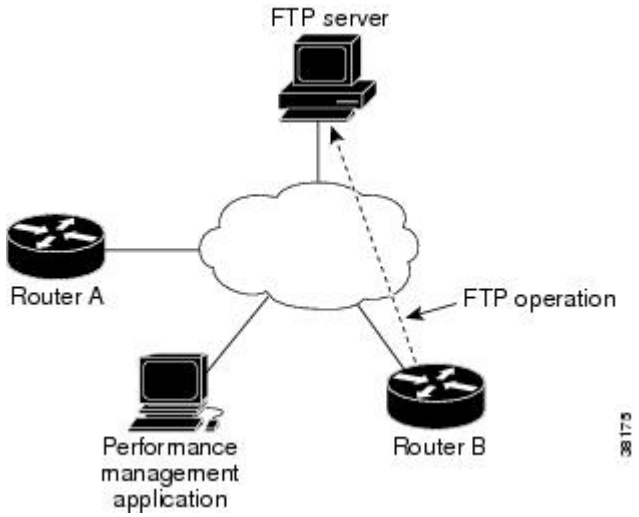
Information About IP SLAs FTP Operations

FTP Operation

The FTP operation measures the round-trip time (RTT) between a Cisco device and an FTP server to retrieve a file. FTP is an application protocol, part of the Transmission Control Protocol (TCP)/IP protocol stack, used for transferring files between network nodes.

In the figure below Device B is configured as the source IP SLAs device and an FTP operation is configured with the FTP server as the destination device.

Figure 15: FTP Operation



Connection response time is computed by measuring the time taken to download a file to Device B from the remote FTP server using FTP over TCP. This operation does not use the IP SLAs Responder.

Note To test the response time to connect to an FTP port (Port 21), use the IP SLAs TCP Connect operation.

Both active and passive FTP transfer modes are supported. The passive mode is enabled by default. Only the FTP GET (download) operation type is supported. The URL specified for the FTP GET operation must be in one of the following formats:

- ftp://username:password@host/filename
- ftp://host/filename

If the username and password are not specified, the defaults are anonymous and test, respectively.

FTP carries a significant amount of data traffic and can affect the performance of your network. The results of an IP SLAs FTP operation to retrieve a large file can be used to determine the capacity of the network but retrieve large files with caution because the FTP operation will consume more bandwidth. The FTP operation also measures your FTP server performance levels by determining the RTT taken to retrieve a file.

How to Configure IP SLAs FTP Operations

Configuring an FTP Operation on a Source Device

Note There is no need to configure an IP SLAs responder on the destination device.

Perform one of the following tasks:

Configuring a Basic FTP Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**}
5. **frequency** *seconds*
6. **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	**ip sla** *operation-number* **Example:** `Device(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	**ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**} **Example:** `Device(config-ip-sla)# ftp get ftp://username:password@hostip/test.cap`	Defines an FTP operation and enters IP SLA FTP configuration mode.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-ftp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**end** **Example:** `Device(config-ip-sla-ftp)# exit`	Exits to privileged EXEC mode.

Configuring an FTP Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**}
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **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	**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	**ftp get** *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**} **Example:** `Device(config-ip-sla)# ftp get ftp://username:password@hostip/filename`	Defines an FTP operation and enters IP SLA FTP configuration mode.
Step 5	**history buckets-kept** *size* **Example:** `Device(config-ip-sla-ftp)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-ftp)# 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:** `Device(config-ip-sla-ftp)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.

	Command or Action	Purpose
Step 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-ftp)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	**frequency** *seconds* **Example:** `Device(config-ip-sla-ftp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-ftp)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-ftp)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	**owner** *owner-id* **Example:** `Device(config-ip-sla-ftp)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-ftp)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	**tag** *text* **Example:** `Device(config-ip-sla-ftp)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-ftp)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 16	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-ftp)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	**end** **Example:** `Device(config-ip-sla-ftp)# end`	Exits to privileged EXEC mode.

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*]}]
	
	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.

	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 FTP Operations

Example: Configuring an FTP Operation

The following example shows how to configure an FTP operation from Device B to the FTP server as shown in the "FTP Operation" figure in the "Information About IP SLAs FTP Operation" section. The operation is scheduled to start every day at 1:30 a.m. In this example, the file named test.cap is to be retrieved from the host, cisco.com, with a password of abc using FTP in active mode.

Device B Configuration

```
ip sla 10
 ftp get ftp://user1:abc@test.cisco.com/test.cap mode active
 frequency 20
 tos 128
 timeout 40000
 tag FLL-FTP
ip sla schedule 10 start-time 01:30:00 recurring
```

Additional References

Related Documents

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

Standards

Standards	Title
ITU-T G.711 u-law and G.711 a-law	Pulse code modulation (PCM) of voice frequencies
ITU-T G.729A	Reduced complexity 8 kbit/s CS-ACELP speech codec

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

RFCs

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

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

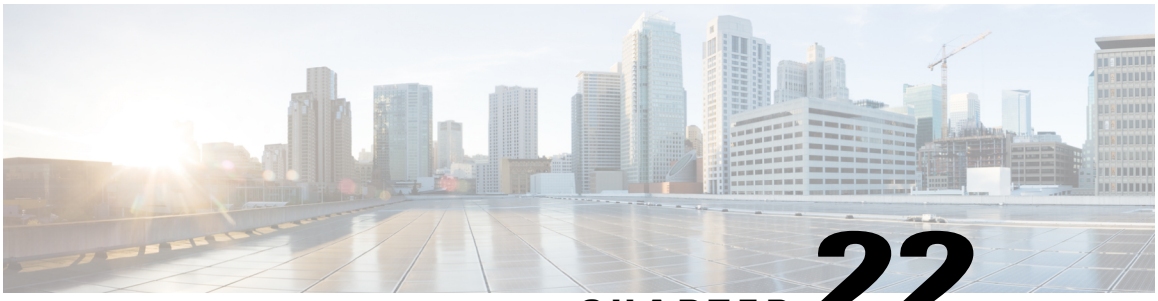
Feature Information for Configuring IP SLAs FTP Operations

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 35: Feature Information for the IP SLAs FTP Operation

Feature Name	Releases	Feature Information
IP SLAs - FTP Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE Release 3.1.0SG	The IP SLAs File Transfer Protocol (FTP) operation allows you to measure the network response time between a Cisco device and an FTP server to retrieve a file.
IPSLA 4.0 - IP v6 phase2	15.2(3)T 15.2(4)S Cisco IOS XE release XE 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: **ftp get** (IP SLA), **show ip sla configuration**, **show ip sla summary**.
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 22

Configuring IP SLAs DNS Operations

This module describes how to configure the IP Service Level Agreements (SLAs) Domain Name System (DNS) operation to measure the difference between the time taken to send a DNS request and receive a reply. This module also demonstrates how the results of the DNS operation can be displayed and analyzed to determine the DNS lookup time which is a critical element for determining the performance of a DNS or web server.

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.

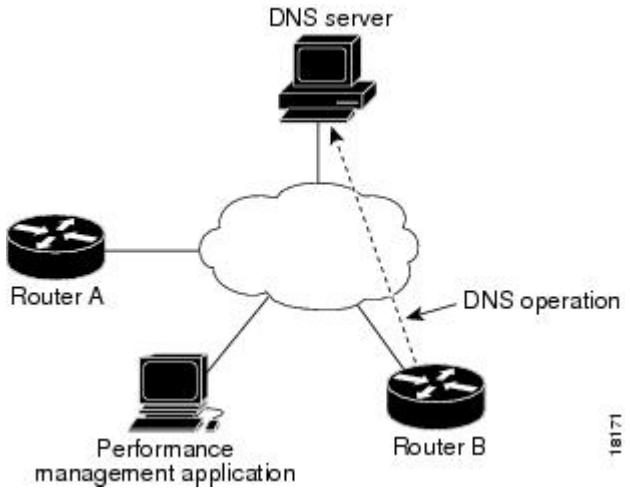
Information About IP SLAs DNS Operations

DNS Operation

The DNS operation measures the difference between the time taken to send a DNS request and receive a reply. DNS is used in the Internet for translating names of network nodes into addresses. The IP SLAs DNS operation queries for an IP address if you specify a host name, or queries for a host name if you specify an IP address.

In the figure below Device B is configured as the source IP SLAs device and a DNS operation is configured with the DNS server as the destination device.

Figure 16: DNS Operation



Connection response time is computed by measuring the difference between the time taken to send a request to the DNS server and the time a reply is received by Device B. The resulting DNS lookup time can help you analyze your DNS performance. Faster DNS lookup times translate to a faster web server access experience.

How to Configure IP SLAs DNS Operations

Configuring an IP SLAs DNS Operation on the Source Device

Note There is no need to configure an IP SLAs responder on the destination device.

Perform one of the following tasks:

Configuring a Basic DNS Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*]
5. **frequency** *seconds*
6. **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	**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	**dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] **Example:** `Device(config-ip-sla)# dns host1 name-server 172.20.2.132`	Defines a DNS operation and enters IP SLA DNS configuration mode.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-dns)# frequency 60`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-ip-sla-dns)# end`	Exits to privileged EXEC mode.

Configuring a DNS Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **end**

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	**dns** {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] **Example:** `Device(config-ip-sla)# dns host1 name-server 172.20.2.132`	Defines a DNS operation and enters IP SLA DNS configuration mode.
Step 5	**history buckets-kept** *size* **Example:** `Device(config-ip-sla-dns)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-dns)# 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:** `Device(config-ip-sla-dns)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-dns)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.

	Command or Action	Purpose
Step 9	**frequency** *seconds* **Example:** `Device(config-ip-sla-dns)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-dns)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-dns)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	**owner** *owner-id* **Example:** `Device(config-ip-sla-dns)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-dns)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	**tag** *text* **Example:** `Device(config-ip-sla-dns)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-dns)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	**timeout** *milliseconds* **Example:** `Device(config-ip-sla-dns)# 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 17	**end** **Example:** `Device(config-ip-sla-dns)# end`	Exits to privileged EXEC mode.

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** *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*]}]
	
	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 DNS Operations

Example Configuring a DNS Operation

The following example shows how to configure a DNS operation from Device B to the DNS server (IP address 172.20.2.132) as shown in the "DNS Operation" figure in the "DNS Operation" section. The operation is scheduled to start immediately. In this example, the target address is a hostname and the DNS operation will query the DNS server for the IP address associated with the hostname host1. No configuration is required at the DNS server.

Device B Configuration

```
ip sla 11
 dns host1 name-server 172.20.2.132
 frequency 50
 timeout 8000
 tag DNS-Test
ip sla schedule 11 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, All Releases

Related Topic	Document Title
Cisco IOS IP SLAs: general information	"Cisco IOS IP SLAs Overview" module of the *Cisco IOS IP SLAs Configuration Guide*.
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" module of the *Cisco IOS P SLAs Configuration Guide*
Proactive threshold monitoring for IP SLAs	"Configuring Proactive Threshold Monitoring of IP SLAs Operations" module of the *Cisco IOS IP SLAs Configuration Guide*

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

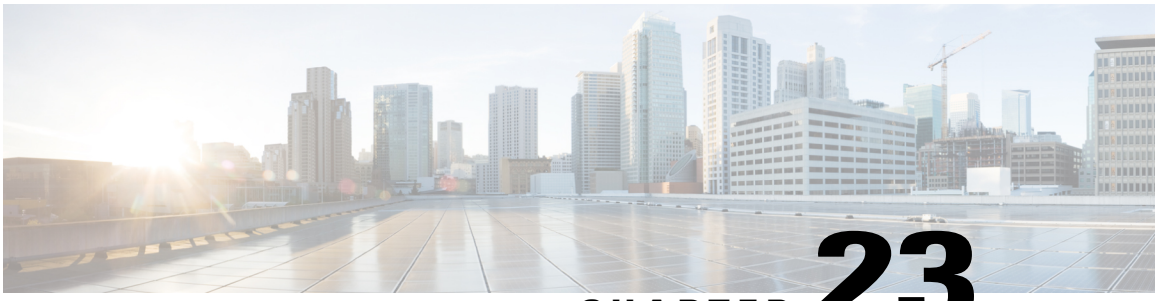
Feature Information for Configuring IP SLAs DNS Operation

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 36: Feature Information for the IP SLAs - DNS Operation

Feature Name	Releases	Feature Information
IP SLAs - DNS Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	The IP SLAs Domain Name System (DNS) Operation feature allows you to measure the difference between the time taken to send a DNS request and receive a reply.
IPSLA 4.0 - IP v6 phase2	15.2(3)T Cisco IOS XE Release 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: **dns (IP SLA)**, **show ip sla configuration**, **show ip sla summary**.
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 23

Configuring IP SLAs DHCP Operations

This module describes how to configure an IP Service Level Agreements (SLAs) Dynamic Host Control Protocol (DHCP) probe to measure the response time between a Cisco device and a DHCP server to obtain an IP address.

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.

Information About IP SLAs DHCP Operations

DHCP Operation

DHCP provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them. The DHCP operation measures the round-trip time (RTT) taken to discover a DHCP server and obtain a leased IP address from it. IP SLAs releases the leased IP address after the operation.

You can use the RTT information to determine DHCP performance levels.

There are two modes for the DHCP operation. By default, the DHCP operation sends discovery packets on every available IP interface on the device. If a specific server is configured on the device, discovery packets are sent only to the specified DHCP server.

IP SLAs DHCP Relay Agent Options

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP device, where IP packets are switched between networks somewhat transparently. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface.

How to Configure IP SLAs DHCP Operations

Note There is no need to configure an IP SLAs responder on the destination device.

Configuring a DHCP Operation on the Source Device

Perform one of the following tasks:

Configuring a Basic DHCP Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **frequency** *seconds*
6. **end**

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	**dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] **Example:** `Device(config-ip-sla)# dhcp 10.10.10.3`	Defines a DHCP operation and enters IP SLA DHCP configuration mode.
Step 5	**frequency** *seconds* **Example:** `Device(config-ip-sla-dhcp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**end** **Example:** `Device(config-ip-sla-dhcp)# end`	Exits to privileged EXEC mode.

Configuring a DHCP Operation with Optional Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history filter** {**none** | **all** | **overThreshold** | **failures**}
8. **frequency** *seconds*
9. **history hours-of-statistics-kept** *hours*
10. **history lives-kept** *lives*
11. **owner** *owner-id*
12. **history statistics-distribution-interval** *milliseconds*
13. **tag** *text*
14. **threshold** *milliseconds*
15. **timeout** *milliseconds*
16. **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	**ip sla** *operation-number* **Example:** `Device(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	**dhcp** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] **Example:** `Device(config-ip-sla)# dhcp 10.10.10.3`	Defines a DHCP operation and enters IP SLA DHCP configuration mode.
Step 5	**history buckets-kept** *size* **Example:** `Device(config-ip-sla-dhcp)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Device(config-ip-sla-dhcp)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Device(config-ip-sla-dhcp)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 8	**frequency** *seconds* **Example:** `Device(config-ip-sla-dhcp)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 9	**history hours-of-statistics-kept** *hours* **Example:** `Device(config-ip-sla-dhcp)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 10	**history lives-kept** *lives* **Example:** `Device(config-ip-sla-dhcp)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 11	**owner** *owner-id* **Example:** `Device(config-ip-sla-dhcp)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.

	Command or Action	Purpose
Step 12	**history statistics-distribution-interval** *milliseconds* **Example:** `Device(config-ip-sla-dhcp)# 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-dhcp)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 14	**threshold** *milliseconds* **Example:** `Device(config-ip-sla-dhcp)# 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-dhcp)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 16	**end** **Example:** `Device(config-ip-sla-dhcp)# end`	Exits to privileged EXEC mode.

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 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`	

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 DHCP Operations

Example Configuration for an IP SLAs DHCP Operation

In the following example, IP SLAs operation number 12 is configured as a DHCP operation enabled for DHCP server 172.16.20.3. Note that DHCP option 82 is used to specify the circuit ID.

Device B Configuration

```
ip dhcp-server 172.16.20.3
!
ip sla 12
 dhcp 10.10.10.3
 frequency 30
 timeout 5000
 tag DHCP_Test
!
ip sla schedule 12 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, All Releases
Cisco IOS IP SLAs: general information	"Cisco IOS IP SLAs Overview" module of the *Cisco IOS IP SLAs Configuration Guide*.
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" module of the *Cisco IOS P SLAs Configuration Guide*
Proactive threshold monitoring for IP SLAs	"Configuring Proactive Threshold Monitoring of IP SLAs Operations" module of the *Cisco IOS IP SLAs Configuration Guide*

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

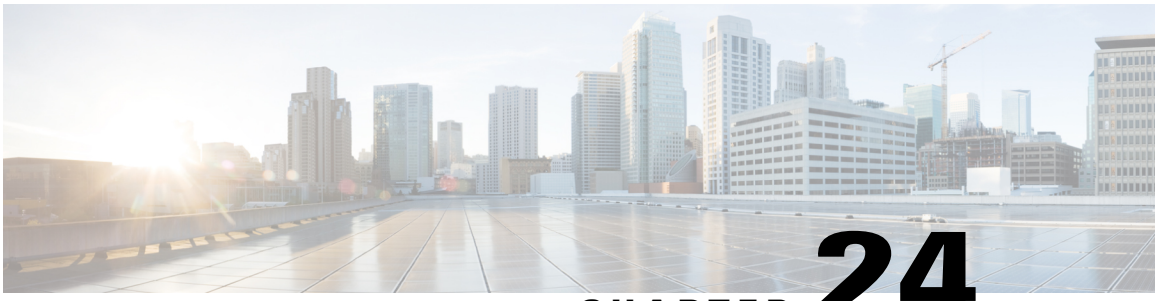
Feature Information for IP SLAs DHCP Operations

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 37: Feature Information for IP SLAs DHCP Operations

Feature Name	Releases	Feature Information
IP SLAs DHCP Probe		The IP SLAs Dynamic Host Control Protocol (DHCP) Probe feature allows you to schedule and measure the network response time between a Cisco device and a DHCP server to obtain an IP address.



CHAPTER 24

Configuring IP SLAs DLSw+ Operations

This module describes how to configure the IP Service Level Agreements (SLAs) Data Link Switching Plus (DLSw+) operation to measure and analyze the DLSw+ protocol stack and network response time between DLSw+ peers.

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.

Prerequisites

A connected DLSw+ peer between the source and destination networking devices must be configured.

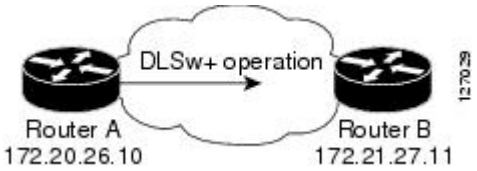
Information About IP SLAs DLSw+ Operations

DLSw+ Operation

The Cisco IOS IP SLAs DLSw+ operation measures the DLSw+ protocol stack and network response time between DLSw+ peers. DLSw+ is the enhanced Cisco version of RFC 1795. DLSw+ tunnels non-routable Layer 2 traffic such as Systems Network Architecture (SNA) traffic over IP backbones via TCP. The networking devices performing the tunneling of non-routable traffic into TCP/IP are referred to as DLSw+ peers. DLSw+ peers normally communicate through TCP port 2065. The destination networking device does not have to be a Cisco router if it supports RFC 1795.

In the figure below, Router A is configured as the source IP SLAs device and a DLSw+ operation is configured with Router B as the remote DLSw+ peer. Router A and Router B are configured as connected DLSw+ peers. The peer (destination device) does not have to run a Cisco IOS IP SLA-capable image.

Figure 17: DLSw+ Operation



Network response time is computed by measuring the round-trip time (RTT) taken to connect to the remote DLSw+ peer using TCP. This operation does not use the IP SLAs Responder.

How to Configure IP SLAs DLSw+ Operations

Configuring IP SLAs DLSw+ Operations

Note There is no need to configure an IP SLAs responder on the destination device.

Perform one of the following tasks:

Configuring a Basic DLSw+ Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dlsw peer-ipaddr** *ip-address*
5. **frequency** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**dlsw peer-ipaddr** *ip-address* **Example:** `Router(config-ip-sla)# dlsw peer-ipaddr 172.21.27.11`	Defines a DLSw+ operation and enters IP SLA DLSw+ configuration mode.
Step 5	**frequency** *seconds* **Example:** `Router(config-ip-sla-dlsw)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**end** **Example:** `Router(config-ip-sla-dlsw)# end`	Exits to privileged EXEC mode.

Configuring an IP SLAs DLSw+ Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **dlsw peer-ipaddr** *ip-address*
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **request-data-size** *bytes*
14. **history statistics-distribution-interval** *milliseconds*
15. **tag** *text*
16. **threshold** *milliseconds*
17. **timeout** *milliseconds*
18. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**dlsw peer-ipaddr** *ip-address* **Example:** `Router(config-ip-sla)# dlsw peer-ipaddr 172.21.27.11`	Defines a DLSw+ operation and enters IP SLA DLSw configuration mode.
Step 5	**history buckets-kept** *size* **Example:** `Router(config-ip-sla-dlsw)# history buckets-kept 25`	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Router(config-ip-sla-dlsw)# 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:** `Router(config-ip-sla-dlsw)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `Router(config-ip-sla-dlsw)# history filter failures`	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	**frequency** *seconds* **Example:** `Router(config-ip-sla-dlsw)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	**history hours-of-statistics-kept** *hours* **Example:** `Router(config-ip-sla-dlsw)# 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 11	**history lives-kept** *lives* **Example:** `Router(config-ip-sla-dlsw)# history lives-kept 5`	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	**owner** *owner-id* **Example:** `Router(config-ip-sla-dlsw)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	**request-data-size** *bytes* **Example:** `Router(config-ip-sla-dlsw)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 14	**history statistics-distribution-interval** *milliseconds* **Example:** `Router(config-ip-sla-dlsw)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 15	**tag** *text* **Example:** `Router(config-ip-sla-dlsw)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 16	**threshold** *milliseconds* **Example:** `Router(config-ip-sla-dlsw)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 17	**timeout** *milliseconds* **Example:** `Router(config-ip-sla-dlsw)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 18	**end** **Example:** `Router(config-ip-sla-dlsw)# exit`	Exits to privileged EXEC mode.

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**]	• 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

	• **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*]}]
	
	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`	

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 SLAs operation is not running and not 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 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 SLAs operation, see the "Configuring Proactive Threshold Monitoring" section.

operation)

To display and interpret the results of an IP SLAs operation, use the **show ip sla statistics** command. Check the output for fields that correspond to criteria in your service level agreement to determine whether the service metrics are acceptable.

Configuration Examples for IP SLAs DLSw+ Operations

Example IP SLAs DLSw+ Operation Configuration

The following example shows the configuration for a DLSw+ operation from Router A to Router B, a remote DLSw+ peer. Router B is configured as a DLSw+ peer and Router A is specified as the remote (connected) DLSw+ peer. Router A is then configured as a DLSw+ peer with Router B as the connected DLSw+ peer, and the IP SLAs DLSw+ operation parameters are configured. The operation is scheduled to start immediately and run for 7200 seconds (2 hours).

Router B Configuration

```
configure terminal
dlsw local-peer peer-id 172.21.27.11
dlsw remote-peer 0 tcp 172.20.26.10
```

Router A Configuration

```
dlsw local-peer peer-id 172.20.26.10
dlsw remote-peer 0 tcp 172.21.27.11
ip sla 14
 dlsw peer-ipaddr 172.21.27.11
 frequency 50
 timeout 50000
 tag DLSw-Test
 exit
ip sla schedule 14 life 7200 start-time now
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Cisco IOS IP SLAs commands	*Cisco IOS IP SLAs Command Reference*
Cisco IOS IP SLAs: general information	Configuring IOS IP SLAs Overview chapter of the *Cisco IOS IP SLAs Configuration Guide*.

Standards

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

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

RFCs

RFCs	Title
RFC 1795	Data Link Switching: Switch-to-Switch Protocol

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

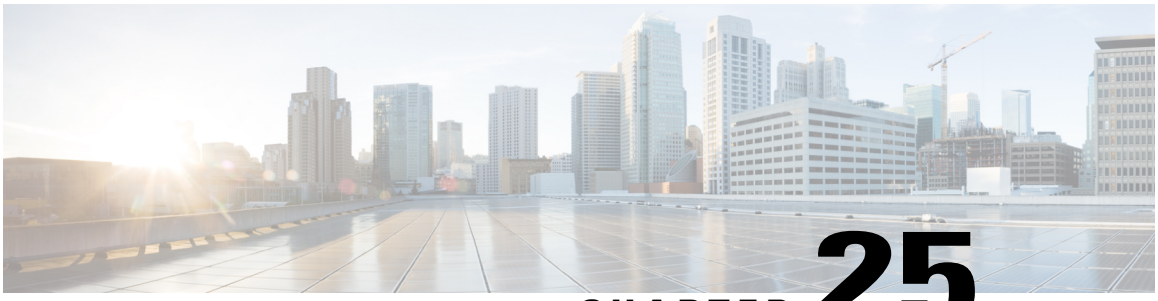
Feature Information for Cisco IOS IP SLAs DLSw+ Operations

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 38: Feature Information for Cisco IOS IP SLAs DLSw+ Operations

Feature Name	Releases	Feature Information
IP SLAs DLSw+ Operation	12.3(14)T 15.0(1)S	The Cisco IOS IP SLAs Data Link Switching Plus (DLSw+) operation allows you to schedule and measure the DLSw+ protocol stack and network response time between DLSw+ peers



CHAPTER 25

Configuring an IP SLAs Multioperation Scheduler

This document describes how to schedule multiple operations at once using the IP Service Level Agreements (SLAs) Multioperations Scheduler feature.

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 an IP SLAs Multioperation Scheduler

Do not use the **no ip sla group schedule** and **ip sla group schedule** commands consecutively in a configuration file and copy it into the running configuration. This causes some of the Service Level Agreement (SLA) probes to go down.

Prerequisites for an IP SLAs Multioperation Scheduler

- Configure the IP SLAs operations to be included in a group before scheduling the group.
- Determine the IP SLAs operations you want to schedule as a single group.
- Identify the network traffic type and the location of your network management station.
- Identify the topology and the types of devices in your network.
- Decide on the frequency of testing for each operation.

Information About an IP SLAs Multioperation Scheduler

IP SLAs Multioperations Scheduler

Normal scheduling of IP SLAs operations allows you to schedule one operation at a time. If you have large networks with thousands of IP SLAs operations to monitor network performance, normal scheduling (scheduling each operation individually) will be inefficient and time-consuming.

Multiple operations scheduling allows you to schedule multiple IP SLAs operations using a single command through the command line interface (CLI) or the CISCO-RTTMON-MIB. This feature allows you to control the amount of IP SLAs monitoring traffic by scheduling the operations to run at evenly distributed times. You must specify the operation ID numbers to be scheduled and the time range over which all the IP SLAs operations should start. This feature automatically distributes the IP SLAs operations at equal intervals over a specified time frame. The spacing between the operations (start interval) is calculated and the operations are started. This distribution of IP SLAs operations helps minimize the CPU utilization and thereby enhances the scalability of the network.

The IP SLAs multiple operations scheduling functionality allows you to schedule multiple IP SLAs operations as a group, using the following configuration parameters:

- Group operation number--Group configuration or group schedule number of the IP SLAs operation to be scheduled.
- Operation ID numbers--A list of IP SLAs operation ID numbers in the scheduled operation group.
- Schedule period--Amount of time for which the IP SLAs operation group is scheduled.
- Ageout--Amount of time to keep the operation in memory when it is not actively collecting information. By default, the operation remains in memory indefinitely.
- Frequency--Amount of time after which each IP SLAs operation is restarted. When the frequency option is specified, it overwrites the operation frequency of all operations belonging to the group. Note that when the frequency option is not specified, the frequency for each operation is set to the value of the schedule period.
- Life--Amount of time the operation actively collects information. The operation can be configured to run indefinitely. By default, the lifetime of an operation is one hour.
- Start time--Time when the operation starts collecting information. You can specify an operation to start immediately or at an absolute start time using hours, minutes, seconds, day, and month.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without aborting. However, this functionality skips those IP SLAs operations that are already running or those that are not configured and hence do not exist. The total number of operations will be calculated based on the number of operations specified in the command, irrespective of the number of operations that are missing or already running. The IP SLAs multiple operations scheduling functionality displays a message showing the number of active and missing operations. However, these messages are displayed only if you schedule operations that are not configured or are already running.

A main benefit for scheduling multiple IP SLAs operations is that the load on the network is reduced by distributing the operations equally over a scheduled period. This distribution helps you to achieve more consistent monitoring coverage. To illustrate this scenario, consider configuring 60 operations to start during the same 1-second interval over a 60-second schedule period. If a network failure occurs 30 seconds after all 60 operations have started and the network is restored before the operations are due to start again (in another 30 seconds), then this failure would never be detected by any of the 60 operations. However, if the 60 operations are distributed equally at 1-second intervals over a 60-second schedule period, then some of the operations would detect the network failure. Conversely, if a network failure occurs when all 60 operations are active, then all 60 operations would fail, indicating that the failure is possibly more severe than it really is.

Operations of the same type and same frequency should be used for IP SLAs multiple operations scheduling. If you do not specify a frequency, the default frequency will be the same as that of the schedule period. The schedule period is the period of time in which all the specified operations should run.

The following sections focus on the interaction of the schedule period and frequency values, additional values, such as start time and lifetime values, are not included in the illustrations.

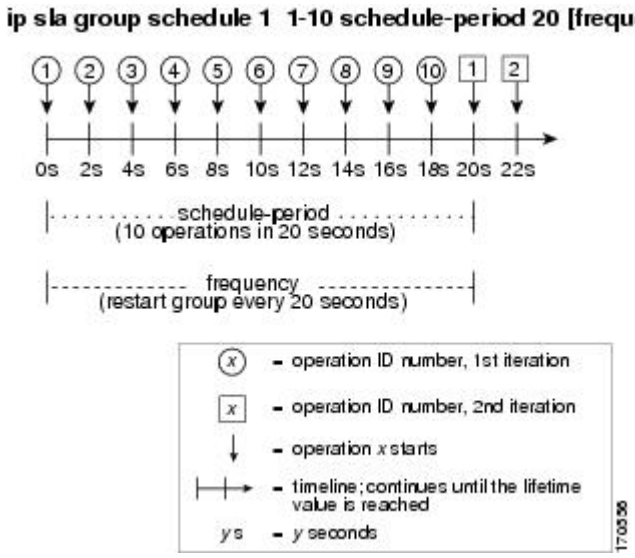
Default Behavior of IP SLAs Multiple Operations Scheduling

The IP SLAs Multiple Operations Scheduling feature allows you to schedule multiple IP SLAs operations as a group.

The figure below illustrates the scheduling of operation group 1 that includes operation 1 to operation 10. Operation group 1 has a schedule period of 20 seconds, which means that all operations in the group will be started at equal intervals within a 20-second period. By default, the frequency is set to the same value as the

configured schedule period. As shown in the figure below, configuring the frequencyis optional because 20 is the default.

Figure 18: Schedule Period Equals Frequency--Default Behavior



In this example, the first operation (operation 1) in operation group 1 will start at 0 seconds. All 10 operations in operation group 1 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

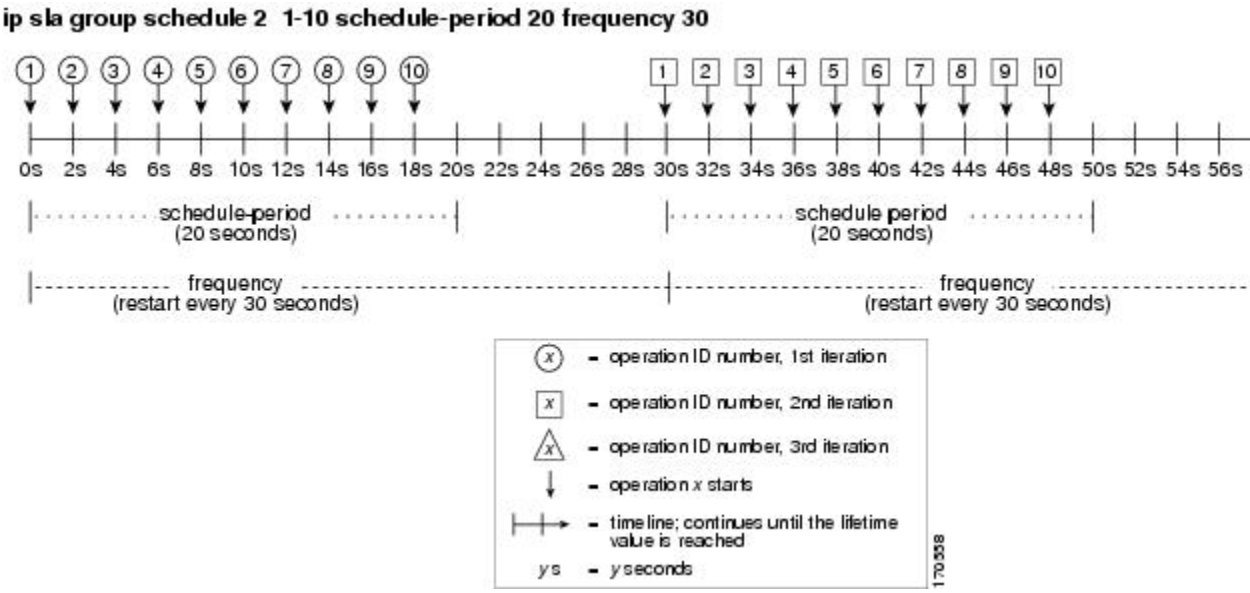
The frequency is the period of time that passes before the operation group is started again (repeated). If the frequency is not specified, the frequency is set to the value of the schedule period. In the example shown above, operation group 1 will start again every 20 seconds. This configuration provides optimal division (spacing) of operations over the specified schedule period.

IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency

The frequency value is the amount of time that passes before the schedule group is restarted, if the schedule period is less than the frequency, there will be a period of time in which no operations are started.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 2. Operation group 2 has a schedule period of 20 seconds and a frequency of 30 seconds.

Figure 19: Schedule Period Is Less Than Frequency



In this example, the first operation (operation 1) in operation group 2 will start at 0 seconds. All 10 operations in operation group 2 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

In the first iteration of operation group 2, operation 1 starts at 0 seconds, and the last operation (operation 10) starts at 18 seconds. However, because the group frequency has been configured to 30 seconds each operation in the operation group is restarted every 30 seconds. So, after 18 seconds, there is a gap of 10 seconds as no operations are started in the time from 19 seconds to 29 seconds. Hence, at 30 seconds, the second iteration of operation group 2 starts. As all ten operations in the operation group 2 must start at an evenly distributed interval in the configured schedule period of 20 seconds, the last operation (operation 10) in the operation group 2 will always start 18 seconds after the first operation (operation 1).

As illustrated in the figure above, the following events occur:

- At 0 seconds, the first operation (operation 1) in operation group 2 is started.
- At 18 seconds, the last operation (operation 10) in operation group 2 is started. This means that the first iteration (schedule period) of operation group 1 ends here.
- From 19 to 29 seconds, no operations are started.
- At 30 seconds, the first operation (operation 1) in operation group 2 is started again. The second iteration of operation group 2 starts here.
- At 48 seconds (18 seconds after the second iteration started) the last operation (operation 10) in operation group 2 is started, and the second iteration of operation group 2 ends.
- At 60 seconds, the third iteration of operation group 2 starts.

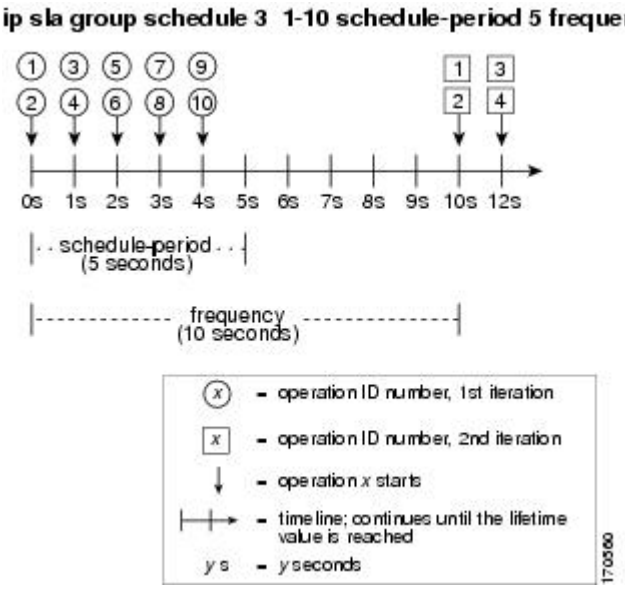
This process continues until the lifetime of operation group 2 ends. The lifetime value is configurable. The default lifetime for an operation group is forever.

Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period

The minimum time interval between the start of IP SLAs operations in a group operation is 1 second. Therefore, if the number of operations to be multiple scheduled is greater than the schedule period, the IP SLAs multiple operations scheduling functionality will schedule more than one operation to start within the same 1-second interval. If the number of operations getting scheduled does not equally divide into 1-second intervals, then the operations are equally divided at the start of the schedule period with the remaining operations to start at the last 1-second interval.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 3. Operation group 3 has a schedule period of 5 seconds and a frequency of 10 seconds.

Figure 20: Number of IP SLAs Operations Is Greater Than the Schedule Period--Even Distribution



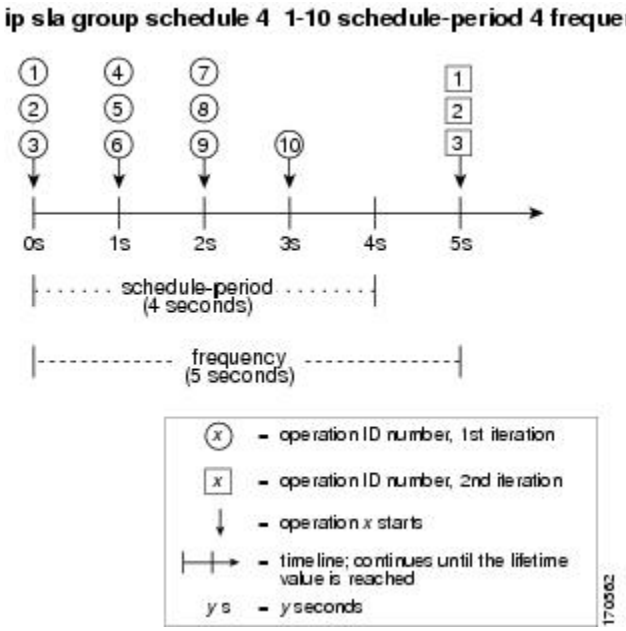
In this example, when dividing the schedule period by the number of operations (5 seconds divided by 10 operations, which equals one operation every 0.5 seconds) the start time of each IP SLAs operation is less than 1 second. Since the minimum time interval between the start of IP SLAs operations in a group operation is 1 second, the IP SLAs multiple operations scheduling functionality instead calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (10 operations divided by 5 seconds). Therefore, as shown in the figure above, two operations will be started every 1 second.

As the frequency is set to 10 in this example, each iteration of operation group 3 will start 10 seconds after the start of the previous iteration. However, this distribution is not optimal as there is a gap of 5 seconds (frequency minus schedule period) between the cycles.

If the number of operations getting scheduled does not equally divide into 1-second intervals, then the operations are equally divided at the start of the schedule period with the remaining operations to start at the last 1-second interval.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 4. Operation group 4 has a schedule period of 4 seconds and a frequency of 5 seconds.

Figure 21: Number of IP SLAs Operations Is Greater Than the Schedule Period--Uneven Distribution



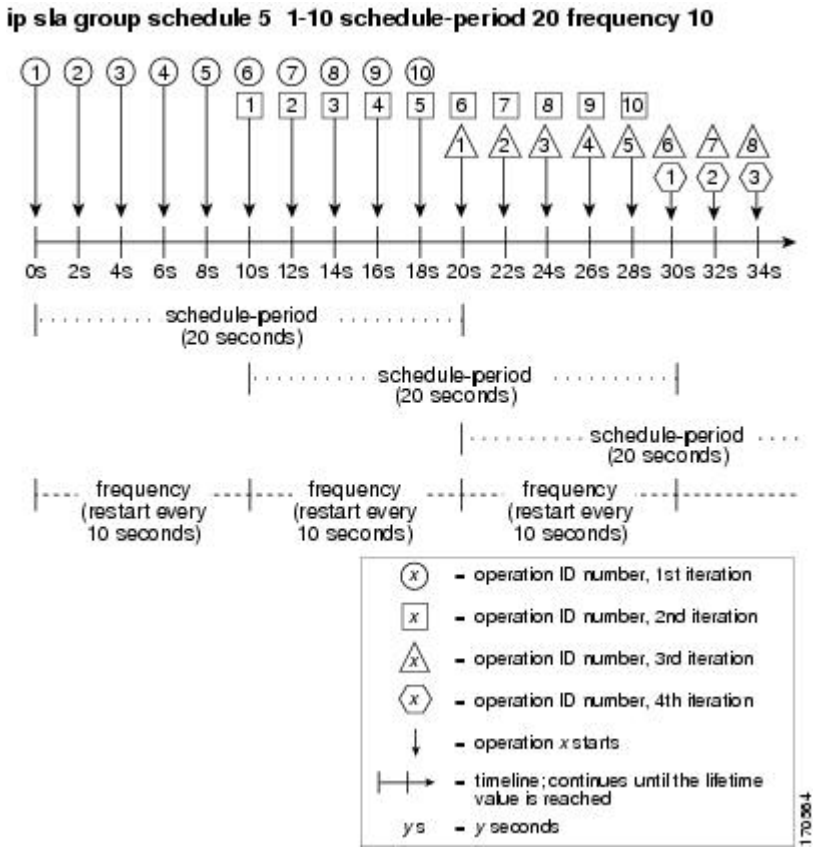
In this example, the IP SLAs multiple operations scheduling functionality calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (10 operations divided by 4 seconds, which equals 2.5 operations every 1 second). Since the number of operations does not equally divide into 1-second intervals, this number will be rounded off to the next whole number (see the figure above) with the remaining operations to start at the last 1-second interval.

IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency

The value of frequency is the amount of time that passes before the schedule group is restarted. If the schedule period is greater than the frequency, there will be a period of time in which the operations in one iteration of an operation group overlap with the operations of the following iteration.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 5. Operation group 5 has a schedule period of 20 seconds and a frequency of 10 seconds.

Figure 22: IP SLAs Group Scheduling with Schedule Period Greater Than Frequency



In this example, the first operation (operation 1) in operation group 5 will start at 0 seconds. All 10 operations in operation group 5 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

In the first iteration of operation group 5, operation 1 starts at 0 seconds, and operation 10, the last operation in the operation group, starts at 18 seconds. Because the operation group is configured to restart every 10 seconds (**frequency 10**), the second iteration of operation group 5 starts again at 10 seconds, before the first iteration is completed. Therefore, an overlap of operations 6 to 10 of the first iteration occurs with operations 1 to 5 of the second iteration during the time period of 10 to 18 seconds (see the figure above). Similarly, there is an overlap of operations 6 to 10 of the second iteration with operations 1 to 5 of the third iteration during the time period of 20 to 28 seconds.

In this example, the start time of operation 1 and operation 6 need not be at exactly the same time, but will be within the same 2-second interval.

The configuration described in this section is not recommended as you can configure multiple operations to start within the same 1-second interval by configuring the number of operations greater than the schedule

period. For information, see the "Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period" section.

IP SLAs Random Scheduler

The IP SLAs Random Scheduler feature is an enhancement to the existing IP SLAs Multioperation Scheduling feature. The IP SLAs Multioperation Scheduling feature provides the capability to easily schedule multiple IP SLAs operations to begin at intervals equally distributed over a specified duration of time and to restart at a specified frequency. With the IP SLAs Random Scheduler feature, you can now schedule multiple IP SLAs operations to begin at random intervals uniformly distributed over a specified duration of time and to restart at uniformly distributed random frequencies within a specified frequency range. Random scheduling improves the statistical metrics for assessing network performance.

Note The IP SLAs Random Scheduler feature is not in compliance with RFC2330 because it does not account for inter-packet randomness.

The IP SLAs random scheduler option is disabled by default. To enable the random scheduler option, you must set a frequency range when configuring a group schedule in global configuration mode. The group of operations restarts at uniformly distributed random frequencies within the specified frequency range. The following guidelines apply for setting the frequency range:

- The starting value of the frequency range should be greater than the timeout values of all the operations in the group operation.
- The starting value of the frequency range should be greater than the schedule period (amount of time for which the group operation is scheduled). This guideline ensures that the same operation does not get scheduled more than once within the schedule period.

The following guidelines apply if the random scheduler option is enabled:

- The individual operations in a group operation will be uniformly distributed to begin at random intervals over the schedule period.
- The group of operations restarts at uniformly distributed random frequencies within the specified frequency range.
- The minimum time interval between the start of each operation in a group operation is 100 milliseconds (0.1 seconds). If the random scheduler option is disabled, the minimum time interval is 1 second.
- Only one operation can be scheduled to begin at any given time. If the random scheduler option is disabled, multiple operations can begin at the same time.
- The first operation will always begin at 0 milliseconds of the schedule period.
- The order in which each operation in a group operation begins is random.

How to Configure an IP SLAs Multioperation Scheduler

Scheduling Multiple IP SLAs Operations

Note

- All IP SLAs operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group should be the same.
- 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 (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**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. **exit**
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	**ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] [**frequency** *group-operation-frequency*] [**life**{**forever**	*seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh:mm:ss*}]	Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.

	Command or Action	Purpose
	Example: `Device(config)# ip sla group schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to the privileged EXEC mode.
Step 5	**show ip sla group schedule** **Example:** `Device# show ip sla group schedule`	(Optional) Displays the IP SLAs group schedule details.
Step 6	**show ip sla configuration** **Example:** `Device# show ip sla configuration`	(Optional) Displays the IP SLAs configuration details.

Enabling the IP SLAs Random Scheduler

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla group schedule** *group-operation-number operation-id-numbers* **schedule-period** *seconds* [**ageout** *seconds*] [**frequency** [*seconds*| **range** *random-frequency-range*]] [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]
4. **exit**

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 group schedule** *group-operation-number operation-id-numbers* **schedule-period** *seconds* [**ageout** *seconds*] [**frequency** [*seconds*| **range** *random-frequency-range*]] [**life**{**forever** | *seconds*}] [**start-time**{*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}] **Example:** `Device(config)# ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100`	Specifies the scheduling parameters of a group of IP SLAs operations. • To enable the IP SLAs random scheduler option, you must configure the **frequency range** *random-frequency-range* keywords and argument.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying IP SLAs Multiple Operations Scheduling

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip sla statistics** **Example:** `Device# show ip sla statistics`	(Optional) Displays the IP SLAs operation details.

	Command or Action	Purpose
Step 2	**show ip sla group schedule** **Example:** `Device# show ip sla group schedule`	(Optional) Displays the IP SLAs group schedule details.
Step 3	**show ip sla configuration** **Example:** `Device# show ip sla configuration`	(Optional) Displays the IP SLAs configuration details.

Examples

After you have scheduled the multiple IP SLAs operations, you can verify the latest operation details using the appropriate **show** commands.

The following example schedules IP SLAs operations 1 through 20 in the operation group 1 with a schedule period of 60 seconds and a life value of 1200 seconds. By default, the frequency is equivalent to the schedule period. In this example, the start interval is 3 seconds (schedule period divided by number of operations).

```
Device# ip sla group schedule 1 1-20 schedule-period 60 life 1200
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla group schedule** command.

```
Device# show ip sla group schedule
Group Entry Number: 1
Probes to be scheduled: 1-20
Total number of probes: 20
Schedule period: 60
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla configuration** command. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE).

```
Device# show ip sla configuration 1
Entry number: 1
Owner:
Tag:
Type of operation to perform: udpEcho
Target address: 10.2.31.121
Source address: 0.0.0.0
Target port: 9001
Source port: 0
Request size (ARR data portion): 16
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
```

```
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Group Scheduled : TRUE
```

The following example shows the latest operation start time of the scheduled multiple IP SLAs operation, when the operations are scheduled at equal intervals, using the **show ip sla statistics** command:

```
Device# show ip sla statistics | include Latest operation start time
Latest operation start time: *03:06:21.760 UTC Tue Oct 21 2003
Latest operation start time: *03:06:24.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:27.751 UTC Tue Oct 21 2003
Latest operation start time: *03:06:30.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:33.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:36.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:39.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:42.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:45.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:48.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:51.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:54.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:57.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:00.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:03.754 UTC Tue Oct 21 2003
Latest operation start time: *03:07:06.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:09.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:12.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:15.755 UTC Tue Oct 21 2003
Latest operation start time: *03:07:18.752 UTC Tue Oct 21 2003
```

Configuration Examples for an IP SLAs Multioperation Scheduler

Example Scheduling Multiple IP SLAs Operations

The following example shows how to scheduls IP SLAs operations 1 to 10 in the operation group 1 with a schedule period of 20 seconds. By default, the frequency is equivalent to the schedule period.

```
Device# ip sla group schedule 1 1-10 schedule-period 20
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla group schedule** command. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE).

```
Device# show ip sla group schedule
Multi-Scheduling Configuration:
Group Entry Number: 1
Probes to be scheduled: 1-10
Schedule period :20
Group operation frequency: 20
Multi-scheduled: TRUE
```

Example Enabling the IP SLAs Random Scheduler

The following example shows how to schedule IP SLAs operations 1 to 3 as a group (identified as group 2). In this example, the operations are scheduled to begin at uniformly distributed random intervals over a schedule period of 50 seconds. The first operation is scheduled to start immediately. The interval is chosen from the specified range upon every invocation of the probe. The random scheduler option is enabled and the uniformly distributed random frequencies at which the group of operations will restart is chosen within the range of 80-100 seconds.

```
ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100 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, All Releases
Cisco IOS IP SLAs: general information	"Cisco IOS IP SLAs Overview" module of the *Cisco IOS IP SLAs Configuration Guide*.
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" module of the *Cisco IOS P SLAs Configuration Guide*
Proactive threshold monitoring for IP SLAs	"Configuring Proactive Threshold Monitoring of IP SLAs Operations" module of the *Cisco IOS IP SLAs Configuration Guide*

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

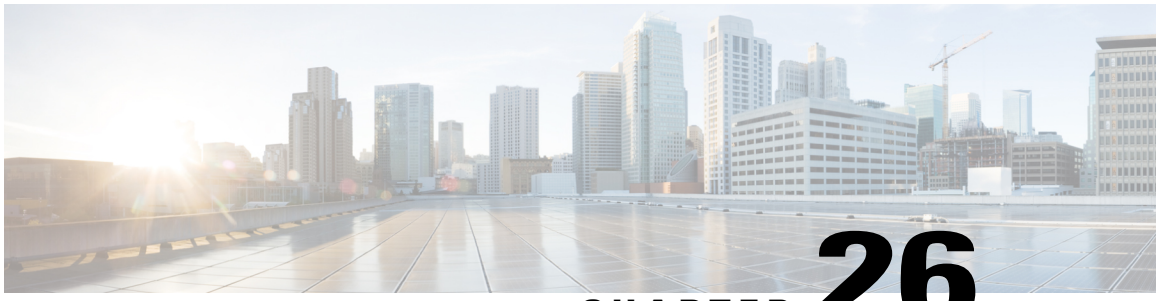
Feature Information for a IP SLAs Multioperation Scheduler

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 39: Feature Information for IP SLAs Multioperation Scheduling

Feature Name	Releases	Feature Information
IP SLAs Multioperation Scheduler		The IP SLAs Multioperation Scheduler feature provides a highly scalable infrastructure for IP SLAs by allowing you to schedule multiple IP SLAs operations using a single command.
IP SLAs Random Scheduler		The IP SLAs Random Scheduler feature provides the capability to schedule multiple IP SLAs operations to begin at random intervals uniformly distributed over a specified duration of time and to restart at uniformly distributed random frequencies within a specified frequency range.



CHAPTER 26

Configuring Proactive Threshold Monitoring for IP SLAs Operations

This document describes the proactive monitoring capabilities of IP Service Level Agreements (SLAs) using thresholds and reaction triggering.

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.

Information About Proactive Threshold Monitoring

IP SLAs Reaction Configuration

IP SLAs reactions are configured to trigger when a monitored value exceeds or falls below a specified level or when a monitored event, such as a timeout or connection loss, occurs. If IP SLAs measures too high or too

low of any configured reaction, IP SLAs can generate a notification to a network management application or trigger another IP SLA operation to gather more data.

When an IP SLA operation is triggered, the (triggered) target operation starts and continues to run independently and without knowledge of the condition of the triggering operation. The target operation continues to run until its life expires, as specified by the target operation's configured lifetime value. The target operation must finish its life before it can be triggered again.

In Cisco IOS Release 15.2(3) and later releases, the (triggered) target operation runs until the condition-cleared event. After which the target operation gracefully stops and the state of the target operation changes from Active to Pending so it can be triggered again.

Supported Reactions by IP SLAs Operation

The tables below list which reactions are supported for each IP SLA operation.

Table 40: Supported Reaction Configuration, by IP SLA Operation

Reaction	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
Failure	Y	--	Y	Y	Y	Y	--	Y	Y	--
RTT	Y	Y	--	Y	Y	Y	Y	--	Y	Y
RTTAvg	--	--	Y	--	--	--	--	Y	--	--
timeout	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
connectionLoss	--	--	Y	Y	Y	--	--	--	--	
verifyError	--	--	Y	Y	--	--	--	Y	--	Y
jitterSDAvg	--	--	Y	--	--	--		Y	--	--
jitterAvg	--	--	Y	--	--	--	--	Y	--	--
packetLateArrival	--	--	Y	--	--	--	--	Y	--	--
packetOutOfSequence	--	--	Y	--	--	--	--	Y	--	--
MaxOfPositivesSD	--	--	Y	--	--	--		Y	--	--
MaxOfNegativesSD	--	--	Y	--	--	--	--	Y	--	--
MaxOfPositivesDS	--	--	Y	--	--	--	--	Y	--	--
MaxOfNegativesDS	--	--	Y	--	--	--	--	Y	--	--
MOS	--	--	Y	--	--	--		--	--	--
ICPIF	--	--	Y	--	--	--	--	--	--	--

Reaction	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
PacketLossDS	--	--	Y	--	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--		--	--	--
iaJitterDS	--	--	--	--	--	--	--	--	--	--
frameLossDS	--	--	--	--	--	--	--	--	--	--
mosLQDSS	--	--	--	--	--	--	--	--	--	--
mosCQDS	--	--	--	--	--	--	--	--	--	--
rfactorDS	--	--	--	--	--	--	--	--	--	--
iaJitterSD	--	--	--	--	--	--	--	--	--	--
successivePackLoss	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	Y	--	--
LatencyDS	--	--	--	--	--	--	--	Y	--	--
LatencySD	--	--	--	--	--	--	--	Y	--	--
packetLoss	--	--	--	--	--	--	--	Y	--	--

Table 41: Supported Reaction Configuration, by IP SLA Operation

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
Failure	--	--	--	--	--	--	--	--	--
RTT	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTTAvg	--	--	--	--	--	--	--	--	--
timeout	Y	Y	Y	Y	--	Y	Y	Y	Y
connectionLoss	Y		Y	Y	Y	--	--	Y	--
verifyError	--	--	--	--	--	--	--	--	--

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
jitterSDAvg	--	--	--	--	--	--	Y	--	--
jitterAvg	--	--	--	--	--	--	Y	--	--
packetLateArrival	--	--	--	--	--	--	Y	--	--
packetOutOfSequence	--	--	--	--	--	--	Y	--	--
MaxOfPositivesSD	--	--	--	--	--	--	Y	--	--
MaxOfNegativesSD	--	--	--	--	--	--	Y	--	--
MaxOfPositivesDS	--	--	--	--	--	--	Y	--	--
MaxOfNegativesDS	--	--	--	--	--	--	Y	--	--
MOS	--	--	--	--	--	--	--	--	--
ICPIF	--	--	--	--	--	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--	--	--	--
iaJitterDS	--	--	Y	--	--	--	--	--	--
frameLossDS	--	--	Y	--	--	--	--	--	--
mosLQDSS	--	--	Y	--	--	--	--	--	--
mosCQDS	--	--	Y	--	--	--	--	--	--
rfactorDS	--	--	Y						
iaJitterSD	--	--	Y	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	--	--
LatencyDS	--	--	--	--	--	--	--	--	--
LatencySD	--	--	--	--	--	--	--	--	--

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
packetLoss	--	--	--	--	--	--	--	--	--

IP SLAs Threshold Monitoring and Notifications

IP SLAs supports proactive threshold monitoring and notifications for performance parameters such as average jitter, unidirectional latency, bidirectional round-trip time (RTT), and connectivity for most IP SLAs operations. The proactive monitoring capability also provides options for configuring reaction thresholds for important VoIP related parameters including unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring.

Notifications for IP SLAs are configured as a triggered reaction. Packet loss, jitter, and Mean Operation Score (MOS) statistics are specific to IP SLAs jitter operations. Notifications can be generated for violations in either direction (source-to-destination and destination-to-source) or for out-of-range RTT values for packet loss and jitter. Events, such as traps, are triggered when the RTT value rises above or falls below a specified threshold.

IP SLAs can generate system logging (syslog) messages when a reaction condition occurs. System logging messages can be sent as Simple Network Management Protocol (SNMP) traps (notifications) using the CISCO-RTTMON-MIB. SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB.

Severity levels in the CISCO-SYSLOG-MIB are defined as follows: SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)}

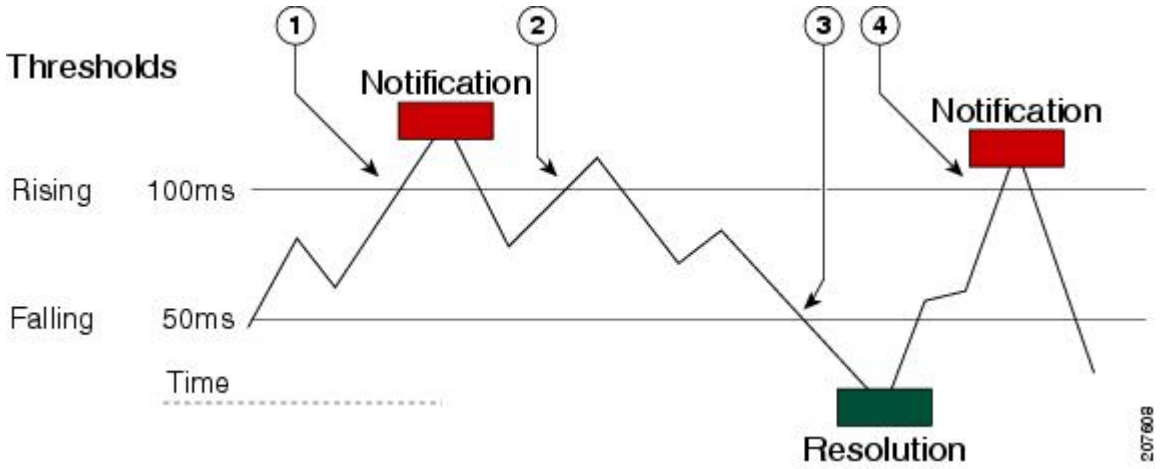
The values for severity levels are defined differently for the system logging process in software. Severity levels for the system logging process in Cisco software are defined as follows: {emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debugging (7)}.

IP SLAs Threshold violations are logged as level 6 (informational) within the Cisco system logging process but are sent as level 7 (info) traps from the CISCO-SYSLOG-MIB.

Notifications are not issued for every occurrence of a threshold violation. The figure below illustrates the sequence for a triggered reaction that occurs when the monitored element exceeds the upper threshold. An event is sent and a notification is issued when the rising threshold is exceeded for the first time. Subsequent

threshold-exceeded notifications are issued only after the monitored value falls below the falling threshold before exceeding the rising threshold ag ain .

Figure 23: IP SLAs Triggered Reaction Condition and Notifications for Threshold Exceeded



1	An event is sent and a threshold-exceeded notification is issued when the rising threshold is exceeded for the first time.
2	Consecutive over-rising threshold violations occur without issuing additional notifications.
3	The monitored value goes below the falling threshold.
4	Another threshold-exceeded notification is issued when the rising threshold is exceeded only after the monitored value first fell below the falling threshold.

Note A lower-threshold notification is also issued the first time that the monitored element falls below the falling threshold (3). As described, subsequent notifications for lower-threshold violations will be issued only after the rising threshold is exceeded before the monitored value falls below the falling threshold again.

RTT Reactions for Jitter Operations

RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT), which matches the value of the average return-trip time (RTTAvg).

SNMP traps for RTT for jitter operations are based on the value of the average return-trip time (RTTAvg) for the whole operation and do not include RTT values for each individual packet sent during the operation. For example, if the average is below the threshold, up to half of the packets can actually be above threshold but this detail is not included in the notification because the value is for the whole operation only.

Only syslog messages are supported for RTTAvg threshold violations. Syslog nmessages are sent from the CISCO-RTTMON-MIB.

How to Configure Proactive Threshold Monitoring

Configuring Proactive Threshold Monitoring

Perform this task to configure thresholds and reactive triggering for generating traps or starting another operation.

Before You Begin

- IP SLAs operations to be started when violation conditions are met must be configured.

Note

- RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).
- SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation. Only syslog messages are supported for RTTAvg threshold violations.
- Only syslog messages are supported for RTT violations during Jitter operations.
- Only SNMP traps are supported for RTT violations during non-Jitter operations.
- Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.
- Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]
4. **ip sla reaction-trigger** *operation-number target-operation*
5. **ip sla logging traps**
6. Do one of the following:
   - **snmp-server enable traps rtr**
   - **snmp-server enable traps syslog**
7. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
8. **exit**
9. **show ip sla reaction- configuration** [*operation-number*]
10. **show ip sla reaction- trigger** [*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 reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*]	**consecutive** [*occurrences*]	**immediate**	**never**	**xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*] **Example:** `Device(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger`	Configures the action (SNMP trap or IP SLAs trigger) that is to occur based on violations of specified thresholds.

	Command or Action	Purpose
Step 4	**ip sla reaction-trigger** *operation-number target-operation* **Example:** `Device(config)# ip sla reaction-trigger 10 2`	(Optional) Starts another IP SLAs operation when the violation conditions are met. • Required only if the **ip sla reaction-configuration** command is configured with either the **trapAndTrigger**or **triggerOnly**keyword.
Step 5	**ip sla logging traps** **Example:** `Device(config)# ip sla logging traps`	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.

Step 6	Do one of the following:
	• **snmp-server enable traps rtr**
	• **snmp-server enable traps syslog**
	Example:
	`Device(config)# snmp-server enable traps rtr`
	Example:
	`Device(config)# snmp-server enable traps syslog`
		• (Optional) The first example shows how to enable the system to generate CISCO-RTTMON-MIB traps.
		• (Optional) The second example shows how to enable the system to generate CISCO-SYSLOG-MIB traps.

Step 7	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Device(config)# snmp-server host 10.1.1.1 public syslog`	(Optional) Sends traps to a remote host. • Required if the **snmp-server enable traps** command is configured.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	**show ip sla reaction- configuration** [*operation-number*] **Example:** `Device# show ip sla reaction-configuration 10`	(Optional) Displays the configuration of proactive threshold monitoring.

	Command or Action	Purpose
Step 10	**show ip sla reaction- trigger** [*operation-number*] **Example:** `Device# show ip sla reaction-trigger 2`	(Optional) Displays the configuration status and operational state of target operations to be triggered.

Configuration Examples for Proactive Threshold Monitoring

Example Configuring an IP SLAs Reaction Configuration

In the following example, IP SLAs operation 10 is configured to send an SNMP logging trap when the MOS value either exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
Device(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

The following example shows the default configuration for the **ip sla reaction-configuration** command:

```
Device# show ip sla reaction-configuration 1
Entry number: 1
Reaction Configuration not configured
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip sla reaction-configuration 1
Device(config)# do show ip sla reaction-configuration 1
Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
```

Example Verifying an IP SLAs Reaction Configuration

The following example shows that multiple monitored elements are configured for the IP SLAs operation (1), as indicated by the values of Reaction: in the output:

```
Device# show ip sla reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
Reaction: jitterDSAvg
Threshold type: average
```

```
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly
Reaction: jitterDSAvg
Threshold type:  immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
Reaction: PacketLossSD
Threshold type:  immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

Example Triggering SNMP Notifications

The following example shows how to configure proactive threshold monitoring so that CISCO-SYSLOG-MIB traps are sent to the remote host at 10.1.1.1 if the threshold values for RTT or VoIP MOS are violated:

```
! Configure the operation on source.
Device(config)# ip sla 1

Device(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
Device(config-ip-sla-jitter)# exit

Device(config)# ip sla schedule 1 start now life forever

! Configure thresholds and reactions.
Device(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly

Device(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly

Device(config)# ip sla logging traps

! The following command sends traps to the specified remote host.
Device(config)# snmp-server host 10.1.1.1 version 2c public syslog

! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
Device(config)# snmp-server enable traps syslog
```

The following sample system logging messages shows that IP SLAs threshold violation notifications are generated as level 6 (informational) in the Cisco system logging process:

```
3d18h:%RTT-6-SAATHRESHOLD:RTR(11):Threshold exceeded for MOS
```

This following sample SNMP notification from the CISCO-SYSLOG-MIB for the same violation is a level 7 (info) notification:

```
3d18h:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
 sysUpTime.0 = 32613038
 snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
 clogHistoryEntry.2.71 = RTT
 clogHistoryEntry.3.71 = 7
 clogHistoryEntry.4.71 = SAATHRESHOLD
```

```
clogHistoryEntry.5.71 = RTR(11):Threshold exceeded for MOS
clogHistoryEntry.6.71 = 32613037
```

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

MIBs

MIBs	MIBs Link
• CISCO-RTTMON-MIB • CISCO-SYSLOG-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

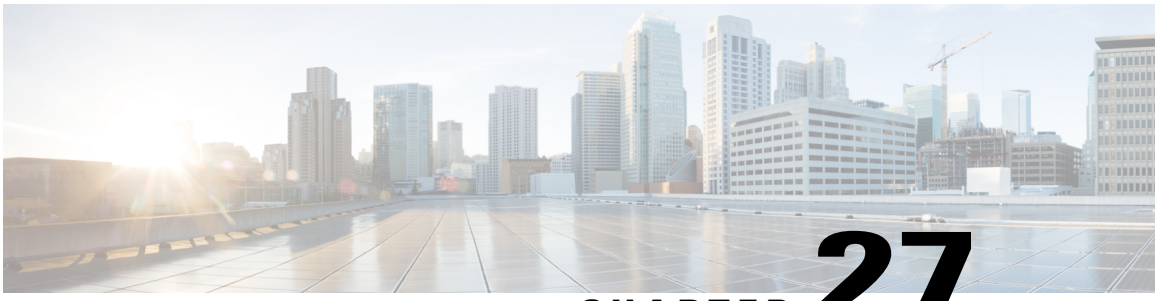
Feature Information for IP SLAs Proactive Threshold Monitoring

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 42: Feature Information for IP SLAs Proactive Threshold Monitoring

Feature Name	Releases	Feature Information
IP SLAs - Reaction Threshold		Cisco IOS IP SLAs proactive threshold monitoring capability allows you to configure an IP SLAs operation to react to certain measured network conditions.
IP SLAs - VoIP Traps		The IP SLA - VoIP Traps feature includes new capabilities for configuring reaction thresholds for important VoIP related parameters such as unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring (MOS scores).
IP SLAs Additional Threshold Traps		This enhancement for IP SLAs reaction threshold monitoring includes per direction average jitter, per direction packet loss, maximum positive and negative jitter, and Mean Opinion Score (MOS) traps. The feature also enables one-way latency jitter, packet loss and latency traps within IP SLAs and includes traps for packet loss due to missing in action and late arrivals.



CHAPTER 27

IP SLAs TWAMP Responder

This module describes how to configure an IETF Two-Way Active Measurement Protocol (TWAMP) responder on a Cisco device to measure IP performance between the Cisco device and a non-Cisco TWAMP control device on your network.

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.

Prerequisites for IP SLAs TWAMP Responder

For the IP SLAs TWAMP responder to function, a TWAMP control-client and the session-sender must be configured in your network.

Restrictions for IP SLAs TWAMP Responder

- For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector must be configured on the same Cisco device.
- Time stamping is not supported for TWAMP test packets that ingress/egress via management interface.
- Time stamping is not supported on interfaces that are not routed or BDI interfaces.
- Time stamping is not supported on MPLS/VPLS interfaces.
- TWAMP client and session sender is not supported.
- Upto nine session-senders can be configured for one TWAMP responder.
- TWAMP Light mode is not supported.

Information About IP SLAs TWAMP Responder

TWAMP

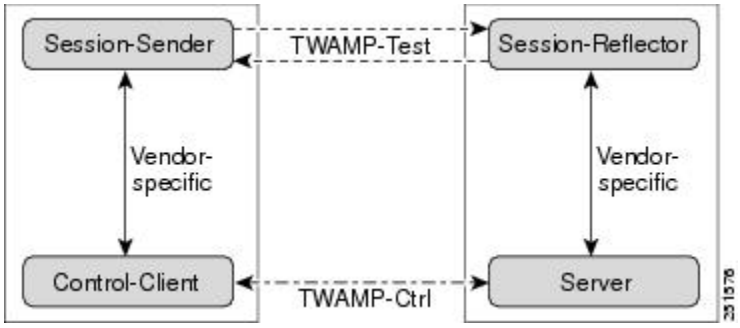
The IETF Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the TWAMP protocols. The TWAMP-Control protocol is used to set up performance measurement sessions. The TWAMP-Test protocol is used to send and receive performance-measurement probes.

The TWAMP architecture is composed of the following four logical entities that are responsible for starting a monitoring session and exchanging packets:

- The control-client sets up, starts, and stops TWAMP-Test sessions.
- The session-sender instantiates TWAMP-Test packets that are sent to the session-reflector.
- The session-reflector reflects a measurement packet upon receiving a TWAMP-Test packet. The session reflector does not collect packet statistics in TWAMP.
- The TWAMP server is an end system that manages one or more TWAMP sessions and is also capable of configuring per-session ports in the end points. The server listens on the TCP port. The session-refector and server make up the TWAMP responder in an IP SLAs operation.

Although TWAMP defines the different entities for flexibility, it also allows for logical merging of the roles on a single device for ease of implementation. The figure below shows the four entities that make up the TWAMP architecture.

Figure 24: TWAMP Architecture

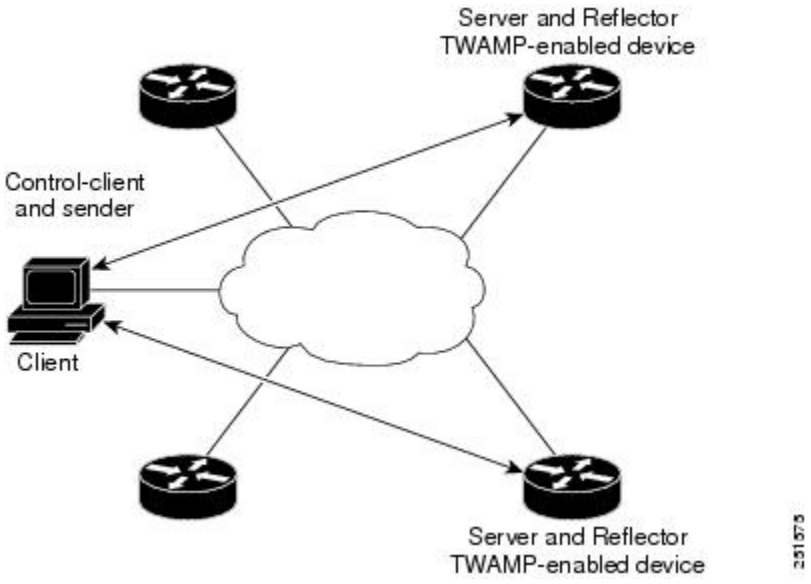


IP SLAs TWAMP Responder v1.0

A TWAMP responder interoperates with the control-client and session-sender on another device that supports TWAMP. In the IP SLAs TWAMP Responder v1.0 feature, the session-reflector and TWAMP server that make up the responder must be co-located on the same device.

In the figure below, one device is the control-client and session-sender (TWAMP control device), and the other two devices are Cisco devices that are configured as IP SLAs TWAMP responders. Each IP SLAs TWAMP responder is both a TWAMP server and a session-reflector.

Figure 25: IP SLAs TWAMP Responders in a Basic TWAMP Deployment



How to Configure an IP SLAs TWAMP Responder

Note Time stamping for sender (T1, T4) and receiver (T3, T2) is performed by hardware, instead of software to improve the accuracy of jitter and latency measurements effective Cisco IOS-XE Everest 16.6.1.

Configuring the TWAMP Server

Note For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector are configured on the same device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla server twamp**
4. **port** *port-number*
5. **timer inactivity** *seconds*
6. **end**

DETAILED STEPS

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 server twamp**

Example:
```
Device(config)#  ip sla server twamp
```

Configures the device as a TWAMP server and enters TWAMP server configuration mode.

Step 4 **port** *port-number*

Example:
```
Device(config-twamp-srvr)# port 9000
```

(Optional) Configures the port to be used by the TWAMP server to listen for connection and control requests.

Step 5 **timer inactivity** *seconds*

Example:
```
Device(config-twamp-srvr)# timer inactivity 300
```

(Optional) Configures the inactivity timer for a TWAMP control session.

Step 6 **end**

Example:
```
Device(config-twamp-srvr)# end
```

Returns to privileged EXEC mode.

Configuring the Session-Reflector

Note For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector are configured on the same device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder twamp**
4. **timeout** *seconds*
5. **end**

DETAILED STEPS

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 responder twamp**

Example:
```
Device(config)# ip sla responder twamp
```

Configures the device as a TWAMP responder and enters TWAMP reflector configuration mode.

Step 4 **timeout** *seconds*

Example:
```
Device(config-twamp-ref)#  timeout 300
```

(Optional) Configures an inactivity timer for a TWAMP test session.

Step 5 **end**

Example:
```
Device(config-twamp-ref)# end
```

Exits to privileged EXEC mode.

Configuration Examples for IP SLAs TWAMP Responder

IP SLAs TWAMP Responder v1.0 Example

The following example and partial output shows how to configure the TWAMP server and the session-reflector for IP SLAs TWAMP Responder v1.0 on the same Cisco device. In this configuration, port 862 is the (default) port to be used by the TWAMP server to listen for connection and control requests. The default port for the server listener is the RFC-specified port and can be reconfigured, if required.

Note In order for the IP SLAs TWAMP responder to function, a control-client and the session-sender must be configured in your network.

```
Device> enable
Device# configure terminal
```

```
Device(config)#  ip sla server twamp
Device(config-twamp-srvr)#  exit
Device(config)#  ip sla responder twamp
Device(config-twamp-ref)# end
Device> show running-config
.
.
.
ip sla responder
ip sla responder twamp
ip sla server twamp
port 862
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 5357	*Two-Way Active Measurement Protocol (TWAMP)*
RFC 4656	*One-way Active Measurement Protocol (OWAMP)*

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 TWAMP Responder

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 43: Feature Information for IP SLAs TWAMP Responder

Feature Name	Releases	Feature Information
IP SLAs TWAMP Responder v1.0	15.2(3)T	This feature enables you to configure the TWAMP server and the session-reflector on a Cisco device for measuring the round-trip performance between an IP SLAs TWAMP responder and a non-Cisco TWAMP control device in your network. The following commands were introduced or modified: **ip sla responder twamp**, **ip sla server twamp**, **port (twamp)**, **show ip sla standards**, **show ip sla twamp connection**, **show ip sla twamp session**, **show ip sla twamp standards**, **timer inactivity**, **timeout (twamp)**..