



IP SLAs Configuration Guide, Cisco IOS Release 12.2SY

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

IP SLAs Overview 1

Finding Feature Information 1

Information About IP SLAs 1

IP SLAs Technology Overview 2

Service Level Agreements 3

Benefits of IP SLAs 3

Network Performance Measurement Using IP SLAs 4

IP SLAs Operation Types 5

IP SLAs Responder and IP SLAs Control Protocol 5

Response Time Computation for IP SLAs 6

IP SLAs Operation Scheduling 6

IP SLAs Operation Threshold Monitoring 7

MPLS VPN Awareness 7

History Statistics 7

Additional References 8

Configuring IP SLAs UDP Jitter Operations 11

Finding Feature Information 11

Prerequisites 11

Information About IP SLAs UDP Jitter Operations 12

IP SLAs UDP Jitter Operation 12

How to Configure IP SLAs UDP Jitter Operations 13

Configuring the IP SLAs Responder on the Destination Device 13

Configuring and Scheduling a UDP Jitter Operation on the Source Device 14

Configuring and Scheduling a Basic UDP Jitter Operation on the Source Device 14

Troubleshooting Tips 16

What to Do Next 16

Configuring and Scheduling a UDP Jitter Operation with Additional Characteristics 16

Troubleshooting Tips 22

What to Do Next 22

Configuration Examples for IP SLAs UDP Jitter Operations	22
Example Configuring a UDP Jitter Operation	22
Additional References	23
Feature Information for IP SLAs UDP Jitter Operations	24
Configuring IP SLAs LSP Health Monitor Operations	27
Finding Feature Information	27
Prerequisites for LSP Health Monitor Operations	27
Restrictions for LSP Health Monitor Operations	28
Information About LSP Health Monitor Operations	28
Benefits of the LSP Health Monitor	28
How the LSP Health Monitor Works	29
Discovery of Neighboring PE Routers	30
The LSP Discovery Process	31
LSP Discovery Groups	32
IP SLAs LSP Ping and LSP Traceroute Operations	34
Proactive Threshold Monitoring for the LSP Health Monitor	34
Multioperation Scheduling for the LSP Health Monitor	35
How to Configure LSP Health Monitor Operations	36
Configuring an LSP Health Monitor Operation	36
Configuring an LSP Health Monitor Operation without LSP Discovery on a PE Router	36
Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Router	41
Scheduling LSP Health Monitor Operations	46
Troubleshooting Tips	47
What to Do Next	47
Manually Configuring and Scheduling an IP SLAs LSP Ping or LSP Traceroute Operation	48
Troubleshooting Tips	51
What to Do Next	51
Verifying and Troubleshooting LSP Health Monitor Operations	52
Configuration Examples for LSP Health Monitors	54
Example Configuring and Verifying the LSP Health Monitor Without LSP Discovery	54
Example Configuring and Verifying the LSP Health Monitor with LSP Discovery	58
Example Manually Configuring an IP SLAs LSP Ping Operation	61
Additional References	61
Feature Information for LSP Health Monitor Operations	62
Configuring IP SLAs for Metro-Ethernet	65

Finding Feature Information	65
Prerequisites for IP SLAs for Metro-Ethernet	65
Restrictions for IP SLAs for Metro-Ethernet	65
Information About IP SLAs for Metro-Ethernet	66
IP SLAs Ethernet Operation Basics	66
How to Configure IP SLAs for Metro-Ethernet	66
Configuring an IP SLAs Auto Ethernet Operation with Endpoint Discovery on the Source Device	67
Manually Configuring an IP SLAs Ethernet Ping or Jitter Operation on the Source Device	70
Scheduling IP SLAs Operations	73
Troubleshooting Tips	75
What to Do Next	75
Configuration Examples for IP SLAs for Metro-Ethernet	75
Example IP SLAs Auto Ethernet Operation with Endpoint Discovery	75
Example Individual IP SLAs Ethernet Ping Operation	76
Additional References	76
Feature Information for IP SLAs for Metro-Ethernet	77
Configuring IP SLAs UDP Echo Operations	79
Finding Feature Information	79
Restrictions for IP SLAs UDP Echo Operations	79
Information About IP SLAs UDP Echo Operations	79
UDP Echo Operation	80
How to Configure IP SLAs UDP Echo Operations	80
Configuring the IP SLAs Responder on the Destination Device	80
Configuring a UDP Echo Operation on the Source Device	82
Configuring a Basic UDP Echo Operation on the Source Device	82
Configuring a UDP Echo Operation with Optional Parameters on the Source Device	83
Scheduling IP SLAs Operations	88
Troubleshooting Tips	90
What to Do Next	90
Configuration Examples for IP SLAs UDP Echo Operations	90
Example Configuring a UDP Echo Operation	90
Additional References	90
Feature Information for the IP SLAs UDP Echo Operation	91
Configuring IP SLAs HTTP Operations	93

Finding Feature Information	93
Restrictions for IP SLAs HTTP Operations	93
Information About IP SLAs HTTP Operations	93
HTTP Operation	94
How to Configure IP SLAs HTTP Operations	94
Configuring an HTTP GET Operation on the Source Device	94
Configuring a Basic HTTP GET Operation on the Source Device	94
Configuring an HTTP GET Operation with Optional Parameters on the Source Device	96
Configuring an HTTP RAW Operation on the Source Device	99
Scheduling IP SLAs Operations	101
Troubleshooting Tips	103
What to Do Next	103
Configuration Examples for IP SLAs HTTP Operations	103
Example Configuring an HTTP GET Operation	104
Example Configuring an HTTP RAW Operation	104
Example Configuring an HTTP RAW Operation Through a Proxy Server	104
Example Configuring an HTTP RAW Operation with Authentication	105
Additional References	105
Feature Information for IP SLAs HTTP Operations	106
Configuring IP SLAs TCP Connect Operations	109
Finding Feature Information	109
Information About the IP SLAs TCP Connect Operation	109
TCP Connect Operation	109
How to Configure the IP SLAs TCP Connect Operation	110
Configuring the IP SLAs Responder on the Destination Device	110
Configuring and Scheduling a TCP Connect Operation on the Source Device	112
Prerequisites	112
Configuring and Scheduling a Basic TCP Connect Operation on the Source Device	112
Troubleshooting Tips	114
What to Do Next	114
Configuring and Scheduling a TCP Connect Operation with Optional Parameters on the Source Device	114
Troubleshooting Tips	119
What to Do Next	120
Configuration Examples for IP SLAs TCP Connect Operations	120

Example Configuring a TCP Connect Operation	120
Additional References	121
Feature Information for the IP SLAs TCP Connect Operation	122
Configuring IP SLAs ICMP Echo Operations	123
Finding Feature Information	123
Restrictions for IP SLAs ICMP Echo Operations	123
Information About IP SLAs ICMP Echo Operations	123
ICMP Echo Operation	124
How to Configure IP SLAs ICMP Echo Operations	124
Configuring an ICMP Echo Operation	124
Configuring a Basic ICMP Echo Operation on the Source Device	124
Configuring an ICMP Echo Operation with Optional Parameters	126
Scheduling IP SLAs Operations	130
Troubleshooting Tips	132
What to Do Next	132
Configuration Examples for IP SLAs ICMP Echo Operations	132
Example Configuring an ICMP Echo Operation	132
Additional References	133
Feature Information for IP SLAs ICMP Echo Operations	134
Configuring IP SLAs ICMP Path Echo Operations	135
Finding Feature Information	135
Restrictions for IP SLAs ICMP Path Echo Operations	135
Information About IP SLAs ICMP Path Echo Operations	135
ICMP Path Echo Operation	136
How to Configure IP SLAs ICMP Path Echo Operations	136
Configuring an ICMP Path Echo Operation on the Source Device	136
Configuring a Basic ICMP Path Echo Operation on the Source Device	137
Configuring an ICMP Path Echo Operation with Optional Parameters on the Source Device	138
Scheduling IP SLAs Operations	143
Troubleshooting Tips	144
What to Do Next	145
Configuration Examples for IP SLAs ICMP Path Echo Operations	145
Example Configuring an ICMP Path Echo Operation	145
Additional References	146

Feature Information for IP SLAs ICMP Path Echo Operations	147
Configuring IP SLAs ICMP Path Jitter Operations	149
Finding Feature Information	149
Prerequisites for ICMP Path Jitter Operations	149
Restrictions for ICMP Path Jitter Operations	150
Information About IP SLAs ICMP Path Jitter Operations	150
ICMP Path Jitter Operation	150
How to Configure the IP SLAs ICMP Path Jitter Operation	151
Configuring the IP SLAs Responder on a Destination Device	151
Configuring an ICMP Path Jitter Operation on the Source Device	152
Configuring a Basic ICMP Path Jitter Operation	152
Configuring an ICMP Path Jitter Operation with Additional Parameters	154
Scheduling IP SLAs Operations	156
Troubleshooting Tips	158
What to Do Next	158
Configuration Examples for IP SLAs ICMP Path Jitter Operations	158
Example Configuring a Path Jitter Operation	158
Additional References	159
Feature Information for IP SLAs ICMP Path Jitter Operations	160
Configuring IP SLAs FTP Operations	163
Finding Feature Information	163
Restrictions for IP SLAs FTP Operations	163
Information About IP SLAs FTP Operations	163
FTP Operation	164
How to Configure IP SLAs FTP Operations	164
Configuring an FTP Operation on a Source Device	165
Configuring a Basic FTP Operation on the Source Device	165
Configuring an FTP Operation with Optional Parameters on the Source Device	166
Scheduling IP SLAs Operations	169
Troubleshooting Tips	171
What to Do Next	171
Configuration Examples for IP SLAs FTP Operations	171
Example Configuring an FTP Operation	171
Additional References	172
Feature Information for IP SLAs FTP Operations	173

Configuring IP SLAs DNS Operations	175
Finding Feature Information	175
Information About IP SLAs DNS Operations	175
DNS Operation	175
How to Configure IP SLAs DNS Operations	176
Configuring an IP SLAs DNS Operation on the Source Device	176
Configuring a Basic DNS Operation on the Source Device	176
Configuring a DNS Operation with Optional Parameters on the Source Device	178
Scheduling IP SLAs Operations	181
Troubleshooting Tips	183
What to Do Next	183
Configuration Examples for IP SLAs DNS Operations	183
Example Configuring a DNS Operation	183
Additional References	184
Feature Information for IP SLAs DNS Operations	185
Configuring IP SLAs DHCP Operations	187
Finding Feature Information	187
Information About IP SLAs DHCP Operations	187
DHCP Operation	187
IP SLAs DHCP Relay Agent Options	188
How to Configure IP SLAs DHCP Operations	188
Configuring a DHCP Operation on the Source Device	188
Configuring a Basic DHCP Operation	188
Configuring a DHCP Operation with Optional Parameters	189
Scheduling IP SLAs Operations	193
Troubleshooting Tips	195
What to Do Next	195
Configuration Examples for IP SLAs DHCP Operations	195
Example Configuration for an IP SLAs DHCP Operation	195
Additional References	195
Feature Information for IP SLAs DHCP Operations	196
Configuring IP SLAs DLSw+ Operations	199
Finding Feature Information	199
Prerequisites	199
Information About IP SLAs DLSw+ Operations	199

DLSw+ Operation	199
How to Configure IP SLAs DLSw+ Operations	200
Configuring IP SLAs DLSw+ Operations	200
Configuring a Basic DLSw+ Operation on the Source Device	200
Configuring an IP SLAs DLSw+ Operation with Optional Parameters on the Source Device	201
Scheduling IP SLAs Operations	205
Troubleshooting Tips	207
What to Do Next	207
Configuration Examples for IP SLAs DLSw+ Operations	207
Example IP SLAs DLSw+ Operation Configuration	207
Additional References	208
Feature Information for Cisco IOS IP SLAs DLSw+ Operations	209
Configuring an IP SLAs Multioperation Scheduler	211
Finding Feature Information	211
Prerequisites for an IP SLAs Multioperation Scheduler	211
Information About an IP SLAs Multioperation Scheduler	211
IP SLAs Multioperations Scheduler	212
Default Behavior of IP SLAs Multiple Operations Scheduling	213
IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency	214
Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period	215
IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency	216
IP SLAs Random Scheduler	218
How to Configure an IP SLAs Multioperation Scheduler	218
Scheduling Multiple IP SLAs Operations	219
Enabling the IP SLAs Random Scheduler	220
Verifying IP SLAs Multiple Operations Scheduling	221
Configuration Examples for an IP SLAs Multioperation Scheduler	223
Example Scheduling Multiple IP SLAs Operations	223
Example Enabling the IP SLAs Random Scheduler	224
Additional References	224
Feature Information for a Cisco IOS IP SLAs Multioperation Scheduler	225
Configuring Proactive Threshold Monitoring for IP SLAs Operations	227
Finding Feature Information	227
Information About Proactive Threshold Monitoring	227

IP SLAs Reaction Configuration	227
Supported Reactions by IP SLAs Operation	228
IP SLAs Threshold Monitoring and Notifications	231
RTT Reactions for Jitter Operations	232
How to Configure Proactive Threshold Monitoring	233
Configuring Proactive Threshold Monitoring	233
Configuration Examples for Proactive Threshold Monitoring	236
Example Configuring an IP SLAs Reaction Configuration	236
Example Verifying an IP SLAs Reaction Configuration	236
Example Triggering SNMP Notifications	237
Additional References	238
Feature Information for IP SLAs Proactive Threshold Monitoring	239



Last Updated: July 18, 2011

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



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, page 1](#)
- [Information About IP SLAs, page 1](#)
- [Additional References, page 8](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 2](#)
- [Service Level Agreements, page 3](#)
- [Benefits of IP SLAs, page 3](#)
- [Network Performance Measurement Using IP SLAs, page 4](#)
- [IP SLAs Operation Types, page 5](#)
- [IP SLAs Responder and IP SLAs Control Protocol, page 5](#)
- [Response Time Computation for IP SLAs, page 6](#)
- [IP SLAs Operation Scheduling, page 6](#)
- [IP SLAs Operation Threshold Monitoring, page 7](#)

- [MPLS VPN Awareness, page 7](#)
- [History Statistics, page 7](#)

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>.

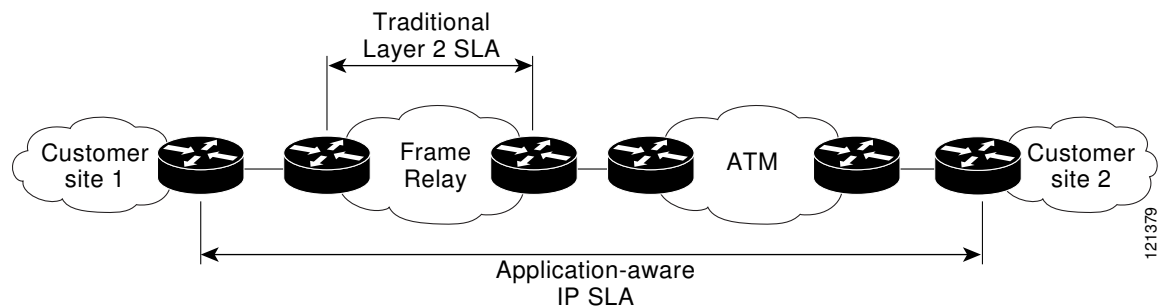
SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and 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



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 routers 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

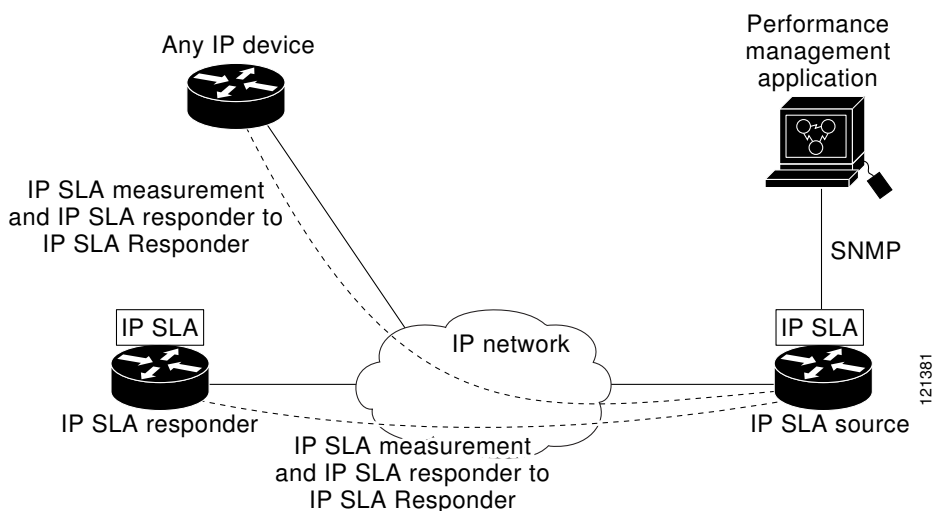
- Provides service level agreement monitoring, measurement, and verification.
- Network performance monitoring
 - Measures the jitter, latency, or packet loss in the network.
 - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment
 - Verifies that the existing 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.

IP SLAs uses generated traffic to measure network performance between two networking devices such as routers. 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



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.

Conceptual information about the IP SLAs Responder and IP SLAs control protocol, the various IP SLAs operation types, thresholding options, and scheduling options are contained in this document.

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 "Cisco IOS XE IP SLAs Operations" in the "Network Performance Measurement Using Cisco IOS XE 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 router (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.

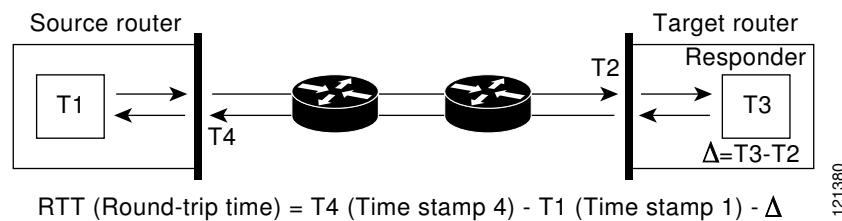
Response Time Computation for IP SLAs

Routers 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 router as well as on the target router (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 router, 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 router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.

Figure 3



An additional benefit of the two time stamps at the target router 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 router and target router 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.

Multiperations 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	<i>Cisco IOS IP SLAs Command Reference</i>

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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 demonstrates how the data gathered using the UDP jitter operation can be displayed and analyzed using the Cisco software commands.

- [Finding Feature Information, page 11](#)
- [Prerequisites, page 11](#)
- [Information About IP SLAs UDP Jitter Operations, page 12](#)
- [How to Configure IP SLAs UDP Jitter Operations, page 13](#)
- [Configuration Examples for IP SLAs UDP Jitter Operations, page 22](#)
- [Additional References, page 23](#)
- [Feature Information for IP SLAs UDP Jitter Operations, page 24](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Time synchronization, such as that provided by NTP, is required between the source and the target device in order to provide accurate one-way delay (latency) measurements. To configure NTP on the source and target devices, perform the tasks in the “Performing Basic System Management” chapter of the *Cisco IOS XE 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.
- 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.

Information About IP SLAs UDP Jitter Operations

- [IP SLAs UDP Jitter Operation, page 12](#)

IP SLAs UDP Jitter Operation

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

Jitter means inter-packet delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (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 the packets arrived greater than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks 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 the data returned by the IP SLAs UDP operation, the UDP jitter operation can be used as a multipurpose data gathering operation. The packets IP SLAs generates carry packet sending sequence and receiving sequence information, and sending and receiving time stamps from the source and the operational target. Based on these, 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 the paths for the sending and receiving of data may be different (asymmetric), the per-direction data allow you to more readily identify where congestion or other problems are occurring in the network.

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

Table 1 *UDP Jitter Operation Parameters*

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

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

How to Configure IP SLAs UDP Jitter Operations

- [Configuring the IP SLAs Responder on the Destination Device, page 13](#)
- [Configuring and Scheduling a UDP Jitter Operation on the Source Device, page 14](#)

Configuring the IP SLAs Responder on the Destination Device

**Note**

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress *ip-address* port *port***
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla responder ip sla responder udp-echo ipaddress <i>ip-address</i> port <i>port</i> <p>Example:</p> <pre>Router(config)# ip sla responder</pre> <p>Example:</p> <pre>Router(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000</pre>	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. or (Optional) Required only if protocol control is disabled on source. Permanently enables IP SLAs Responder functionality on specified IP address and port. <ul style="list-style-type: none"> Control is enabled by default.
Step 4 exit <p>Example:</p> <pre>Router(config)# exit</pre>	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a UDP Jitter Operation on the Source Device

Perform only one of the following tasks:

- [Configuring and Scheduling a Basic UDP Jitter Operation on the Source Device, page 14](#)
- [Configuring and Scheduling a UDP Jitter Operation with Additional Characteristics, page 16](#)

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

SUMMARY STEPS

- enable**
- configure terminal**
- ip sla *operation-number***
- 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*]
- frequency** *seconds*
- exit**
- 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**]
- exit**
- show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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	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: Router(config-ip-sla)# udp-jitter 172.29.139.134 5000	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration submode. <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	frequency seconds Example: Router(config-ip-sla-jitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	exit Example: Router(config-ip-sla-jitter)# exit	Exits UDP jitter configuration submode and returns to global configuration mode.

Command or Action	Purpose
Step 7 <code>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]</code> Example: <pre>Router(config)# ip sla schedule 5 start-time now life forever</pre>	Configures the scheduling parameters for an individual IP SLAs operation.
Step 8 <code>exit</code> Example: <pre>Router(config)# exit</pre>	(Optional) Exits global configuration mode and returns to privileged EXEC mode.
Step 9 <code>show ip sla configuration [operation-number]</code> Example: <pre>Router# show ip sla configuration 10</pre>	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuring and Scheduling a UDP Jitter Operation with Additional Characteristics

**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. 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 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>).

Before configuring a UDP jitter operation on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco 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. **history statistics-distribution-interval** *milliseconds*
12. **tag** *text*
13. **threshold** *milliseconds*
14. **timeout** *milliseconds*
15. Do one of the following:
 - **tos** *number*
 - **traffic-class** *number*
16. **flow-label** *number*
17. **verify-data**
18. **vrf** *vrf-name*
19. **exit**
20. **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**]
21. **exit**
22. **show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • 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	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: Router(config-ip-sla)# udp-jitter 172.29.139.134 5000	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration submode. <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	history distributions-of-statistics-kept size Example: Router(config-ip-sla-jitter)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 6	history enhanced [interval seconds] [buckets number-of-buckets] Example: Router(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: Router(config-ip-sla-jitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 8	history hours-of-statistics-kept <i>hours</i> Example: Router(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 9	owner <i>owner-id</i> Example: Router(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 <i>bytes</i> Example: Router(config-ip-sla-jitter)# request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 11	history statistics-distribution-interval <i>milliseconds</i> Example: Router(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 12	tag <i>text</i> Example: Router(config-ip-sla-jitter)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 13	threshold <i>milliseconds</i> Example: Router(config-ip-sla-jitter)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 14	timeout <i>milliseconds</i> Example: Router(config-ip-sla-jitter)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.

	Command or Action	Purpose
Step 15	<p>Do one of the following:</p> <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# tos 160</pre> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# traffic-class 160</pre>	<p>(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.</p> <p>or</p> <p>(Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.</p>
Step 16	<p>flow-label <i>number</i></p> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# flow-label 112233</pre>	<p>(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.</p>
Step 17	<p>verify-data</p> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# verify-data</pre>	<p>(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.</p>
Step 18	<p>vrf <i>vrf-name</i></p> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# vrf vpn-A</pre>	<p>(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.</p>
Step 19	<p>exit</p> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# exit</pre>	<p>Exits UDP jitter configuration submode and returns to global configuration mode.</p>
Step 20	<p>ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh:mm:ss</i> <i>month day</i> <i>day month</i>} pending now after <i>hh:mm:ss</i>] [ageout <i>seconds</i>] [recurring]</p> <p>Example:</p> <pre>Router(config)# ip sla schedule 5 start-time now life forever</pre>	<p>Configures the scheduling parameters for an individual IP SLAs operation.</p>

Command or Action	Purpose
Step 21 <code>exit</code> Example: <pre>Router(config)# exit</pre>	(Optional) Exits global configuration mode and returns to privileged EXEC mode.
Step 22 <code>show ip sla configuration [operation-number]</code> Example: <pre>Router# show ip sla configuration 10</pre>	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs UDP Jitter Operations

- [Example Configuring a UDP Jitter Operation, page 22](#)

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.

```
ip sla 1
  udp-jitter 20.0.10.3 65051 num-packets 20
  request-data-size 160
  tos 128
```

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

On the target (destination) device:

```
ip sla responder
```

Additional References

Related Documents

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

Standards

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

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 specific RFCs are supported by the features in this document.	--

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

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 2 *Feature Information for IP SLAs UDP Jitter Operations*

Feature Name	Releases	Feature Information
IP SLAs UDP Jitter Operation	12.2(31)SB2	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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SRC	Support was added for operability in IPv6 networks.
	12.2(33)SB	
	12.4(20)T	
	Cisco IOS XE 3.1.0SG	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party

trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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 with LSP Discovery feature. LSP health monitors enable you 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) routers. This end-to-end (PE-to-PE router) 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, page 27](#)
- [Prerequisites for LSP Health Monitor Operations, page 27](#)
- [Restrictions for LSP Health Monitor Operations, page 28](#)
- [Information About LSP Health Monitor Operations, page 28](#)
- [How to Configure LSP Health Monitor Operations, page 36](#)
- [Configuration Examples for LSP Health Monitors, page 54](#)
- [Additional References, page 61](#)
- [Feature Information for LSP Health Monitor Operations, page 62](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 routers of an LSP Health Monitor operation must support the MPLS LSP ping feature. It is recommended that the Provider (P) routers also support the MPLS LSP Ping feature in order to obtain complete error reporting and diagnostics information.
- Ensure that the source PE router has enough memory to support the desired LSP Health Monitor functionality. Enabling the LSP discovery option can potentially have a significant impact on router

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 routers 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, page 28](#)
- [How the LSP Health Monitor Works, page 29](#)
- [Discovery of Neighboring PE Routers, page 30](#)
- [The LSP Discovery Process, page 31](#)
- [LSP Discovery Groups, page 32](#)
- [IP SLAs LSP Ping and LSP Traceroute Operations, page 34](#)
- [Proactive Threshold Monitoring for the LSP Health Monitor, page 34](#)
- [Multioperation Scheduling for the LSP Health Monitor, page 35](#)

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 router. To prevent unnecessary router 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 router 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 Routers" section.

**Note**

By default, only a single path between the source and destination PE routers is discovered. If the LSP discovery option is enabled, the equal-cost multipaths between the source and destination PE routers 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 router and the discovered destination PE router. 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 routers and existing IP SLAs operations are automatically deleted for any PE routers 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 Routers

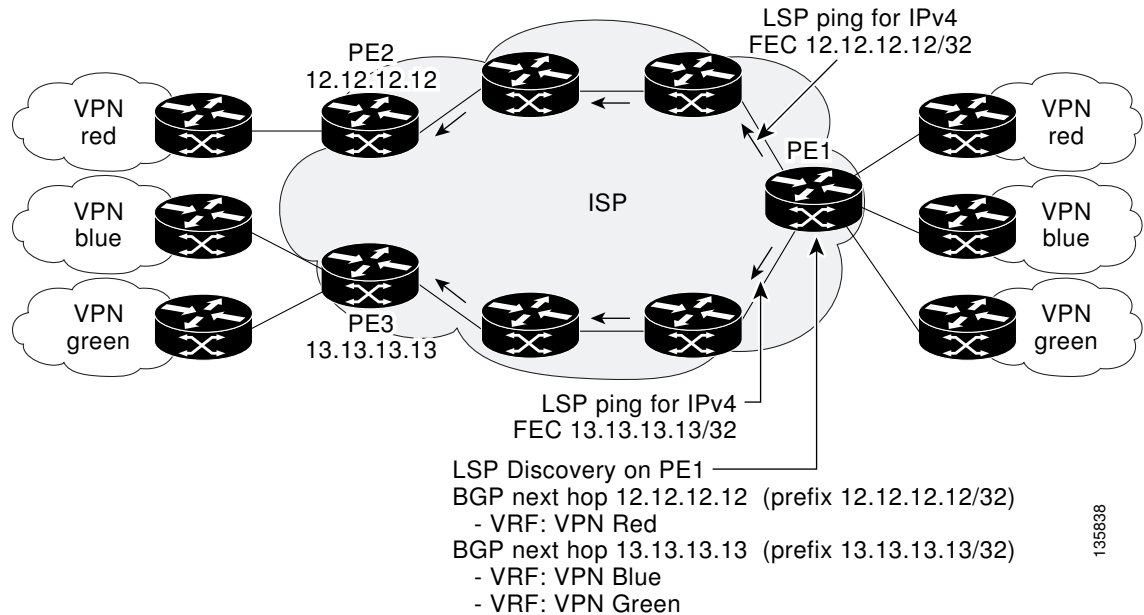
A BGP next hop neighbor discovery process is used to find the BGP next hop neighbors in use by any VRF associated with the source PE router. In most cases, these neighbors will be PE routers.

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 router 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 router PE1: red, blue, and green. From the perspective of router PE1, these VPNs are reachable remotely through BGP next hop neighbors PE2 (router ID: 12.12.12.12) and PE3 (router ID: 13.13.13.13). When the BGP next hop neighbor discovery process is enabled on router PE1, a database is generated based on the local VRF and global routing tables. The database in this example contains two BGP next hop router entries: PE2 12.12.12.12 and PE3 13.13.13.13. The routing entries are maintained per next hop router to distinguish which next hop routers belong within which particular VRF. For each next hop router entry, the IPv4

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

Figure 4



The LSP Discovery Process

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 routers. 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 router 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.

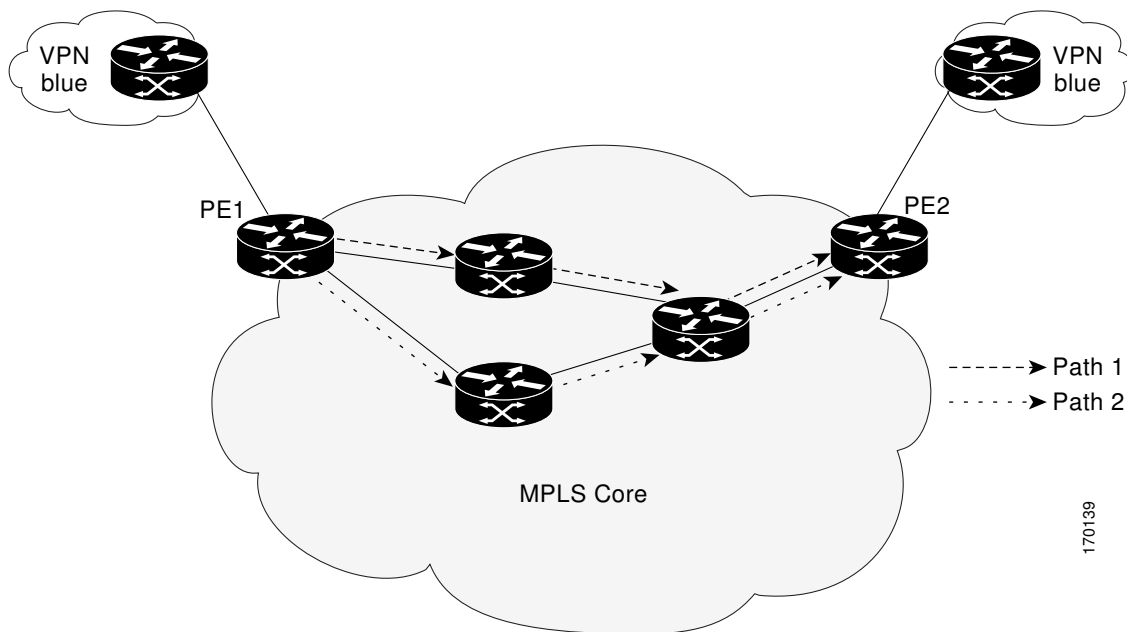
**Note**

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 router and discovered destination PE router. The IP SLAs superoperation operates by sending an LSP ping packet to the destination PE router 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 router 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 router pair, and significantly reduces the number of active LSP ping operations sent by the source PE router.

The figure below illustrates a simple VPN scenario. This network consists of a core MPLS VPN with two PE routers (router PE1 and router PE2) belonging to the VRF named VPN blue. Suppose router PE1 is the source PE router for an LSP Health Monitor operation with the LSP discovery option enabled and that router PE2 is discovered by the BGP discovery process as a BGP next hop neighbor to router PE1. If path 1 and path 2 are equal-cost multipaths between router PE1 to router 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



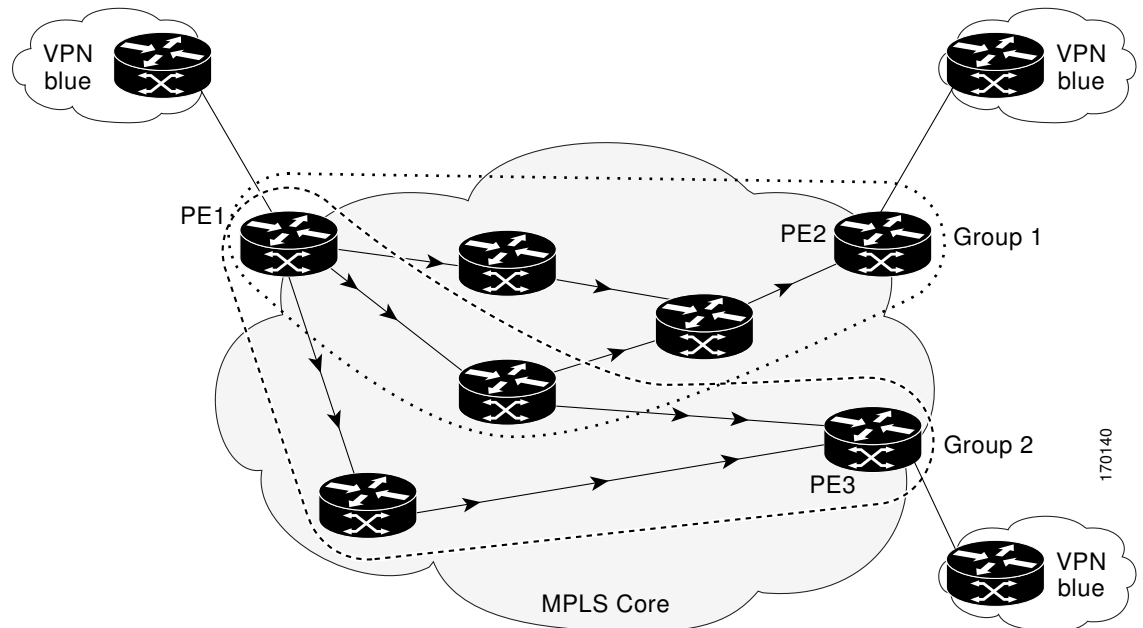
170139

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 routers (router PE1, PE2, and PE3) belonging to the VRF named VPN blue. Suppose router PE1 is the source PE router for an LSP Health Monitor operation with the LSP discovery option enabled and that router PE2 and PE3 are discovered by the BGP discovery process as BGP next hop neighbors to router PE1. LSP discovery group 1 is created for the equal-cost multipaths between router PE1 to router PE2 and LSP discovery group 2 is created for the equal-cost multipaths between router PE1 to router PE3.

Figure 6



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 router and discovered destination PE router. 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 router 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 router 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 Operations

This 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 router and the discovered destination PE routers. 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 option 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 3 *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.

Individual IP SLAs Operation Return Code	Current Group Status = UP	Current Group Status = PARTIAL	Current Group Status = DOWN
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 the 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 router 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 the LSP Health Monitor is similar to configuring a standard multioperation schedule for a group of individual IP SLAs operations.

LSP Discovery Option 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. In other words, initially, network connectivity between the source PE router and discovered destination PE router 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, page 36](#)
- [Scheduling LSP Health Monitor Operations, page 46](#)
- [Manually Configuring and Scheduling an IP SLAs LSP Ping or LSP Traceroute Operation, page 48](#)
- [Verifying and Troubleshooting LSP Health Monitor Operations, page 52](#)

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 Router, page 36](#)
- [Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Router, page 41](#)

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

**Note**

If the LSP discovery option is disabled, only a single path between the source PE router 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.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	mpls discovery vpn next-hop Example: <pre>Router(config)# mpls discovery vpn next-hop</pre>	(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: <pre>Router(config)# mpls discovery vpn interval 120</pre>	(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: <pre>Router(config)# auto ip sla mpls-lsp-monitor 1</pre>	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: <ul style="list-style-type: none"> • type echo [ipsla-vrf-all vrf vpn-name] • type pathEcho [ipsla-vrf-all vrf vpn-name] Example: <pre>Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all</pre> Example: <pre>Router(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all</pre>	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: <pre>Router(config-auto-ip-sla-mpls-params)# access-list 10</pre>	(Optional) Specifies the access list to apply to an LSP Health Monitor operation.

	Command or Action	Purpose
Step 8	scan-interval <i>minutes</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# scan-interval 5</pre>	(Optional) Sets the timer for the IP SLAs LSP Health Monitor database.
Step 9	delete-scan-factor <i>factor</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# delete-scan-factor 2</pre>	(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. <ul style="list-style-type: none"> • 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: <pre>Router(config-auto-ip-sla-mpls-params)# force-explicit-null</pre>	(Optional) Adds an explicit null label to all echo request packets of an IP SLAs operation.
Step 11	exp <i>exp-bits</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# exp 5</pre>	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.
Step 12	lsp-selector <i>ip-address</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# lsp- selector 127.0.0.10</pre>	(Optional) Specifies the local host IP address used to select the LSP of an IP SLAs operation.

Command or Action	Purpose
Step 13 reply-dscp-bits <i>dscp-value</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# reply-dscp-bits 5</pre>	(Optional) Specifies the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation.
Step 14 reply-mode { ipv4 router-alert } Example: <pre>Router(config-auto-ip-sla-mpls-params)# reply-mode router-alert</pre>	(Optional) Specifies the reply mode for an echo request packet of an IP SLAs operation. <ul style="list-style-type: none"> The default reply mode is an IPv4 UDP packet.
Step 15 request-data-size <i>bytes</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# request-data-size 200</pre>	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
Step 16 secondary-frequency { both connection-loss timeout } <i>frequency</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10</pre>	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.
Step 17 tag <i>text</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# tag testgroup</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18 threshold <i>milliseconds</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# threshold 6000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 19	timeout <i>milliseconds</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# timeout 7000</pre>	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
Step 20	ttl <i>time-to-live</i> Example: <pre>Router(config-auto-ip-sla-mpls-params)# ttl 200</pre>	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.
Step 21	exit Example: <pre>Router(config-auto-ip-sla-mpls-params)# exit</pre>	Exits MPLS parameters configuration submode and returns to global configuration mode.
Step 22	auto ip sla mpls-lsp-monitor reaction-configuration <i>operation-number</i> react {connectionLoss timeout} [action-type option] [threshold-type {consecutive [occurrences] immediate never}] Example: <pre>Router(config)# auto ip sla mpls-lsp- monitor reaction-configuration 1 react connectionLoss action-type trapOnly threshold-type consecutive 3</pre>	(Optional) Configures certain actions to occur based on events under the control of the LSP Health Monitor.
Step 23	exit Example: <pre>Router(config)# exit</pre>	Exits global configuration submode and returns to privileged EXEC mode.

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

**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 router. To prevent unnecessary router 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	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	mpls discovery vpn next-hop Example: Router(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: Router(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: Router(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: Router(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 Router" section.
Step 8	path-discover Example: Router(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 submenu.

	Command or Action	Purpose
Step 9	hours-of-statistics-kept <i>hours</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# hours-of-statistics-kept 1</pre>	(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: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# force-explicit-null</pre>	(Optional) Adds an explicit null label to all echo request packets of an LSP Health Monitor operation.
Step 11	interval <i>milliseconds</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# interval 2</pre>	(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.
Step 12	lsp-selector-base <i>ip-address</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# lsp-selector-base 127.0.0.2</pre>	(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 <i>number</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# maximum-sessions 2</pre>	(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 router's CPU.
Step 14	scan-period <i>minutes</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# scan-period 30</pre>	(Optional) Sets the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.
Step 15	session-timeout <i>seconds</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# session-timeout 60</pre>	(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.

	Command or Action	Purpose
Step 16	timeout <i>seconds</i> Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# timeout 4</pre>	(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 router's CPU.
Step 17	exit Example: <pre>Router(config-auto-ip-sla-mpls-lpd-params)# exit</pre>	Exits LSP discovery parameters configuration submode and returns to MPLS parameters configuration mode.
Step 18	exit Example: <pre>Router(config-auto-ip-sla-mpls-params)# exit</pre>	Exits MPLS parameters configuration mode and returns to global configuration mode.
Step 19	auto ip sla mpls-lsp-monitor reaction-configuration <i>operation-number</i> react lpd { lpd-group [retry <i>number</i>] tree-trace } [action-type trapOnly] Example: <pre>Router(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type trapOnly</pre>	(Optional) Configures the proactive threshold monitoring parameters for an LSP Health Monitor operation with LSP discovery enabled.
Step 20	ip sla logging traps Example: <pre>Router(config)# ip sla logging traps</pre>	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
Step 21	exit Example: <pre>Router(config)# exit</pre>	Exits global configuration submode 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 router. 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 multioperation 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.

- 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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
Step 3 auto ip sla mpls-lsp-monitor schedule <i>operation-number</i> schedule-period <i>seconds</i> [frequency <i>seconds</i>] [start-time { after <i>hh : mm : ss</i> <i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] now pending }] Example: Router(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: Router(config)# exit	Exits to privileged EXEC mode.
Step 5 show ip sla configuration Example: Router# show ip sla configuration	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 47](#)
- [What to Do Next, page 47](#)

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	Enables privileged EXEC mode.
	Example:	<ul style="list-style-type: none"> • Enter your password if prompted.
	Router> enable	

	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 1	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> 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: Router(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1 Example: Example: Router(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1	Configures the IP SLAs operation as an LSP ping operation and enters LSP ping configuration mode. or Configures the IP SLAs operation as an LSP trace operation and enters LSP trace configuration mode.
Step 5	exp exp-bits Example: Router(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 <i>bytes</i> Example: Router(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 } <i>frequency</i> Example: Router(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. <ul style="list-style-type: none"> This command is for IP SLAs LSP ping operations only. LSP trace configuration mode does not support this command.
Step 8	tag <i>text</i> Example: Router(config-sla-monitor-lspPing)# tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	threshold <i>milliseconds</i> Example: Router(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 <i>milliseconds</i> Example: Router(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 <i>time-to-live</i> Example: Router(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: Router(config-sla-monitor-lspPing)# exit	Exits LSP ping or LSP trace configuration submode and returns to global configuration mode.

Command or Action	Purpose
<p>Step 13 ip sla reaction-configuration <i>operation-number</i> [react <i>monitored-element</i>] [threshold-type {never immediate consecutive [<i>consecutive-occurrences</i>] xofy [<i>x-value</i> <i>y-value</i>] average [<i>number-of-probes</i>]}] [threshold-value <i>upper-threshold</i> <i>lower-threshold</i>] [action-type {none trapOnly triggerOnly trapAndTrigger}]</p> <p>Example:</p> <pre>Router(config)# ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type traponly</pre>	<p>(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.</p>
<p>Step 14 ip sla logging traps</p> <p>Example:</p> <pre>Router(config)# ip sla logging traps</pre>	<p>(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.</p>
<p>Step 15 ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month</i> <i>day</i> <i>day</i> <i>month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring]</p> <p>Example:</p> <pre>Router(config)# ip sla schedule 1 start-time now</pre>	<p>Configures the scheduling parameters for an IP SLAs operation.</p>
<p>Step 16 exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits global configuration submode and returns to privileged EXEC mode.</p>

- [Troubleshooting Tips, page 51](#)
- [What to Do Next, page 47](#)

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 <i>[operation-number]</i> Example: Router# debug ip sla error	(Optional) Enables debugging output of IP SLAs operation run-time errors.
Step 2	debug ip sla mpls-lsp-monitor <i>[operation-number]</i> Example: Router# debug ip sla mpls-lsp-monitor	(Optional) Enables debugging output of LSP Health Monitor operations.
Step 3	debug ip sla trace <i>[operation-number]</i> Example: Router# 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 <i>[group-id]</i> Example: Router# 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 <i>[operation-number]</i> Example: Router# 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 <i>[group-id]</i> Example: Router# 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: Router# 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 <i>operation-number</i> Example: Router# 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 <i>[operation-number [group [group-id]]]</i> Example: Router# 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 <i>[operation-number] [details]</i> Example: Router# 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.

Command or Action	Purpose
Step 11 <code>show ip sla statistics aggregated [operation-number] [details]</code> Example: Router# <code>show ip sla statistics aggregated 100001</code>	(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.
Step 12 <code>show mpls discovery vpn</code> Example: Router# <code>show mpls discovery vpn</code>	(Optional) Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

Configuration Examples for LSP Health Monitors

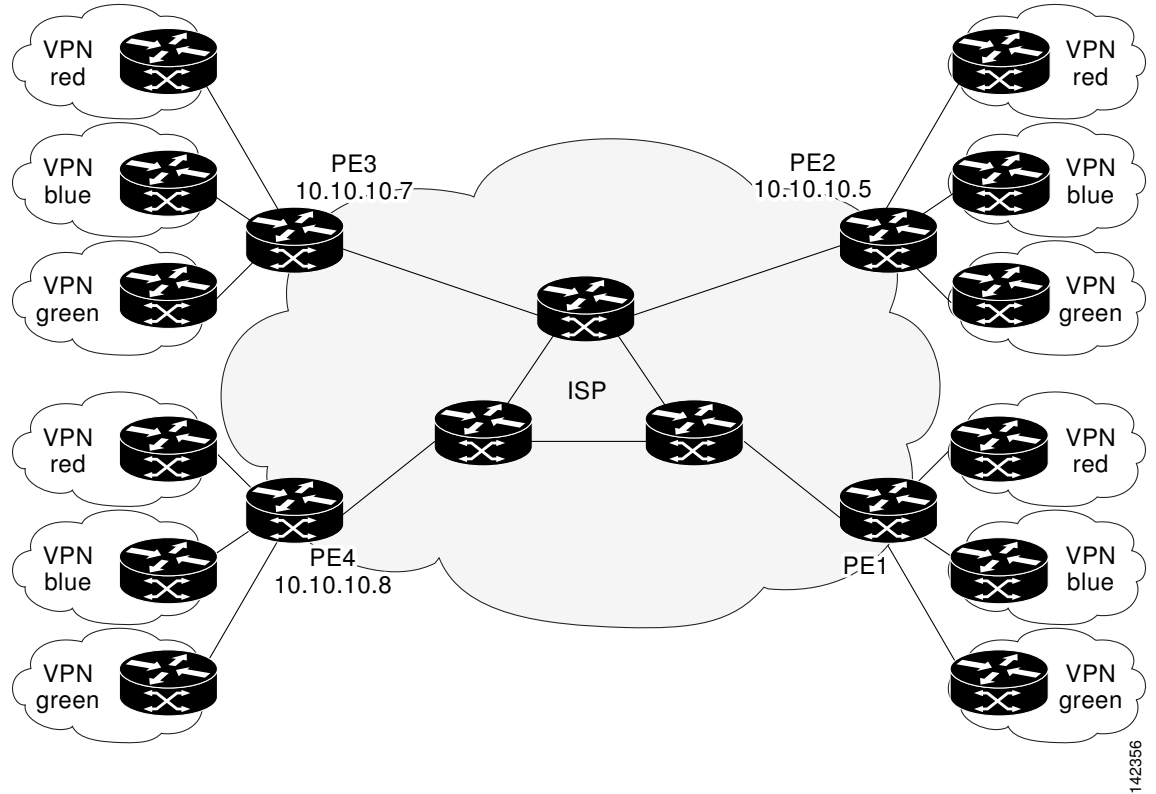
- [Example Configuring and Verifying the LSP Health Monitor Without LSP Discovery, page 54](#)
- [Example Configuring and Verifying the LSP Health Monitor with LSP Discovery, page 58](#)
- [Example Manually Configuring an IP SLAs LSP Ping Operation, page 61](#)

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 routers belonging to three VPNs: red, blue, and green. From the perspective of router PE1,

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

Figure 7



The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on router 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 router 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.

Router 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 router 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 router 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 router 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 router PE1 to router PE4 is lost. This output

shows that connection loss to each of the VPNs associated with router PE4 (red, blue, and green) was detected and that this information was added to the LSP Health Monitor scan queue. Also, since router PE4 is no longer a valid BGP next hop neighbor, the IP SLAs operation for router PE4 (Probe 100003) 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 router PE1 to router PE4 is restored. This output shows that each of the VPNs associated with router PE4 (red, blue, and green) were discovered and that this information was added to the LSP Health Monitor scan queue. Also, since router PE4 is a newly discovered BGP next hop neighbor, a new IP SLAs operation for router PE4 (Probe 100005) is being created and added to the LSP Health Monitor multioperation schedule. Even though router PE4 belongs to three VPNs, only one IP SLAs operation is being created.

```

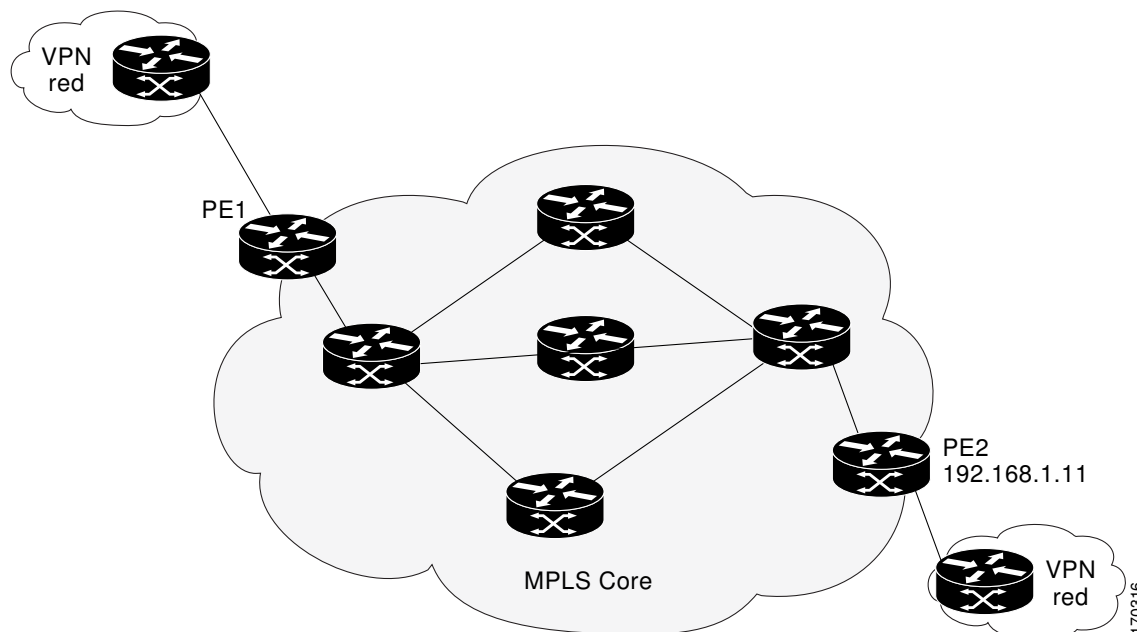
PE1# show ip sla mpls-lsp-monitor scan-queue 1
Next scan Time after: 23 Secs
Next Delete scan Time after: 23 Secs
BGP Next hop      Prefix          vrf          Add/Delete?
10.10.10.8        10.10.10.8/32  red          Add
10.10.10.8        10.10.10.8/32  blue         Add
10.10.10.8        10.10.10.8/32  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 routers belonging to a VPN named red. From the perspective of router PE1, there are three equal-cost multipaths available to reach router PE2.

Figure 8



The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on router 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 router PE1 and router 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.

Router 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 router 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 router 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 router 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 ping and LSP traceroute management tools	MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV chapter of the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>
MPLS LSP discovery management tool	MPLS EM-MPLS LSP Multipath Tree Trace chapter of the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>
Configuring standard IP access lists	Access Control Lists chapter of the <i>Cisco IOS Security Configuration Guide: Securing the Data Plane</i>
Multioperation scheduling for Cisco IOS IP SLAs	Configuring Multioperation Scheduling of IP SLAs Operations chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i>
Proactive threshold monitoring for Cisco IOS IP SLAs	Configuring Proactive Threshold Monitoring of IP SLAs Operations chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	<i>Cisco IOS IP SLAs Command Reference</i>

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)
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

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 4 **Feature Information for the LSP Health Monitor**

Feature Name	Releases	Feature Information
IP SLAs--LSP Health Monitor	12.2(27)SBC	The IP SLAs LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs.
	12.2(28)SB	
	12.2(33)SRA	
	12.4(6)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
IP SLAs--LSP Health Monitor	12.2(31)SB2	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.
	12.2(33)SB	
	12.2(33)SRB	
	12.2(33)SXH	
IP SLAs--LSP Health Monitor with LSP Discovery	12.2(31)SB2	The LSP discovery capability was added.
	12.2(33)SRB	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 65](#)
- [Prerequisites for IP SLAs for Metro-Ethernet, page 65](#)
- [Restrictions for IP SLAs for Metro-Ethernet, page 65](#)
- [Information About IP SLAs for Metro-Ethernet, page 66](#)
- [How to Configure IP SLAs for Metro-Ethernet, page 66](#)
- [Configuration Examples for IP SLAs for Metro-Ethernet, page 75](#)
- [Additional References, page 76](#)
- [Feature Information for IP SLAs for Metro-Ethernet, page 77](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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).

Information About IP SLAs for Metro-Ethernet

- [IP SLAs Ethernet Operation Basics](#), page 66

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:

- Jitter (source-to-destination and destination-to-source)
- 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, page 67](#)
- [Manually Configuring an IP SLAs Ethernet Ping or Jitter Operation on the Source Device, page 70](#)
- [Scheduling IP SLAs Operations, page 73](#)

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	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	ip sla ethernet-monitor <i>operation-number</i> Example: Router(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 <i>domain-name</i> { evc <i>evc-id</i> vlan <i>vlan-id</i> } [exclude-mpids <i>mp-ids</i>] Example: Router(config-ip-sla-ethernet-monitor)# type echo domain testdomain vlan 34	For Echo operations only: Configures an auto Ethernet operation for Ethernet ping operations.
Step 5	type jitter domain <i>domain-name</i> { evc <i>evc-id</i> vlan <i>vlan-id</i> } [exclude-mpids <i>mp-ids</i>] [interval <i>interframe-interval</i>] [num-frames <i>frames-number</i>] Example: Router(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.
Step 6	cos <i>cos-value</i> Example: Router(config-ip-sla-ethernet-params)# cos 2	(Optional) Sets the class of service for an IP SLAs Ethernet operation.
Step 7	owner <i>owner-id</i> Example: Router(config-ip-sla-ethernet-params)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 8	request-data-size <i>bytes</i> Example: Router(config-ip-sla-ethernet-params)# request-data-size 64	(Optional) Sets the padding size for the data frame of an IP SLAs Ethernet operation. <ul style="list-style-type: none"> 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 9	tag <i>text</i> Example: Router(config-ip-sla-ethernet-params)# tag TelnetsPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 10	threshold <i>milliseconds</i> Example: Router(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 <i>milliseconds</i> Example: Router(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: Router(config-ip-sla-ethernet-params)# end	Exits to privileged EXEC configuration mode.
Step 13	show ip sla ethernet-monitor configuration [<i>operation-number</i>] Example: Router# show ip sla ethernet-monitor configuration 1	(Optional) Displays configuration settings for all IP SLAs auto Ethernet operations or a specified auto Ethernet operation.

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	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	ip sla <i>operation-number</i>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
	Example: Router(config)# ip sla 1	

	Command or Action	Purpose
Step 4	ethernet echo mpid <i>mp-id</i> domain <i>domain-name</i> { evc <i>evc-id</i> port vlan <i>vlan-id</i> } Example: Router(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.
Step 5	ethernet jitter mpid <i>mp-id</i> domain <i>domain-name</i> { evc <i>evc-id</i> port vlan <i>vlan-id</i> } [interval <i>interframe-interval</i>] [num-frames <i>frames-number</i>] Example: Router(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.
Step 6	cos <i>cos-value</i> Example: Router(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 the Ethernet echo operation. However, the commands are the same in the Ethernet jitter configuration mode.
Step 7	frequency <i>seconds</i> Example: Router(config-ip-sla-ethernet-echo)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 8	history <i>history-parameter</i> Example: Router(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 <i>owner-id</i> Example: Router(config-ip-sla-ethernet-echo)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.

Command or Action	Purpose
Step 10 <code>request-data-size bytes</code> Example: <pre>Router(config-ip-sla-ethernet-echo)# request- data-size 64</pre>	(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 11 <code>tag text</code> Example: <pre>Router(config-ip-sla-ethernet-echo)# tag TelnetPollSever1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 12 <code>threshold milliseconds</code> Example: <pre>Router(config-ip-sla-ethernet-echo)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 13 <code>timeout milliseconds</code> Example: <pre>Router(config-ip-sla-ethernet-echo)# timeout 10000</pre>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 14 <code>end</code> Example: <pre>Router(config-ip-sla-ethernet-echo)# end</pre>	Exits to privileged EXEC mode.
Step 15 <code>show ip sla configuration [operation-number]</code> Example: <pre>Router# show ip sla configuration 1</pre>	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.
Step 16 <code>show ip sla application</code> Example: <pre>Router# show ip sla application</pre>	(Optional) Displays global information about supported IP SLAs features.

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. **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**}]
4. **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**]
5. **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*}]
6. **exit**
7. **show ip sla group schedule**
8. **show ip sla configuration**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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 ethernet-monitor schedule <i>operation-number</i> schedule-period <i>seconds</i> [frequency <i>[seconds]</i>] [start-time { after <i>hh : mm : ss</i> <i>hh : mm : ss</i>] <i>[month day day month]</i> now pending }] Example: Router(config)# ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now	For individual auto Ethernet operations only: Configures scheduling parameters for an IP SLAs auto Ethernet operation.
Step 4 ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh : mm : ss</i>] <i>[month day day month]</i> pending now after <i>hh : mm : ss</i>] <i>[ageout seconds]</i> [recurring] Example: Router(config)# ip sla schedule 1 start-time now life forever	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation.
Step 5 ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life { forever <i>seconds</i> }] [start-time { <i>hh:mm:ss</i>] <i>[month day day month]</i> pending now after <i>hh:mm:ss</i> }] Example: Router(config)# ip sla group schedule 1 3,4,6-9	For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 6 exit Example: Router(config)# exit	Exits to the privileged EXEC mode.
Step 7 show ip sla group schedule Example: Router# show ip sla group schedule	(Optional) Displays the IP SLAs group schedule details.
Step 8 show ip sla configuration Example: Router# show ip sla configuration	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 75](#)
- [What to Do Next, page 16](#)

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.

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

Configuration Examples for IP SLAs for Metro-Ethernet

- [Example IP SLAs Auto Ethernet Operation with Endpoint Discovery, page 75](#)
- [Example Individual IP SLAs Ethernet Ping Operation, page 76](#)

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	<i>Cisco IOS IP SLAs Command Reference</i>
Ethernet CFM	Configuring Ethernet Connectivity Fault Management in a Service Provider Network module of the <i>Cisco IOS Carrier Ethernet Configuration Guide</i>
Multioperation scheduling for Cisco IOS IP SLAs	Configuring a Multiple Operation Scheduler module of the <i>Cisco IOS IP SLAs Configuration Guide</i>
Proactive threshold monitoring for Cisco IOS IP SLAs	Configuring Proactive Threshold Monitoring of IP SLAs Operations module of the <i>Cisco IOS IP SLAs Configuration Guide</i>

Standards

Standard	Title
IEEE 802.1ag	<i>Connectivity Fault Management</i>

MIBs

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

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 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 5 **Feature Information for IP SLAs for Metro-Ethernet**

Feature Name	Releases	Feature Information
IP SLAs for Metro-Ethernet	12.2(33)SB	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.
	12.2(33)SRB	
	12.2(33)SXI	
	12.4(20)T	
	15.0(1)S	
IP SLAs Metro-Ethernet 2.0 (EVC)	12.2(33)SRD	Support for Ethernet Virtual Circuits (EVCs) was added.
	15.0(1)S	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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 router and devices using IPv4 or IPv6. UDP echo accuracy is enhanced by using the IP SLAs Responder at the destination Cisco router. 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, page 79](#)
- [Restrictions for IP SLAs UDP Echo Operations, page 79](#)
- [Information About IP SLAs UDP Echo Operations, page 79](#)
- [How to Configure IP SLAs UDP Echo Operations, page 80](#)
- [Configuration Examples for IP SLAs UDP Echo Operations, page 90](#)
- [Additional References, page 90](#)
- [Feature Information for the IP SLAs UDP Echo Operation, page 91](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

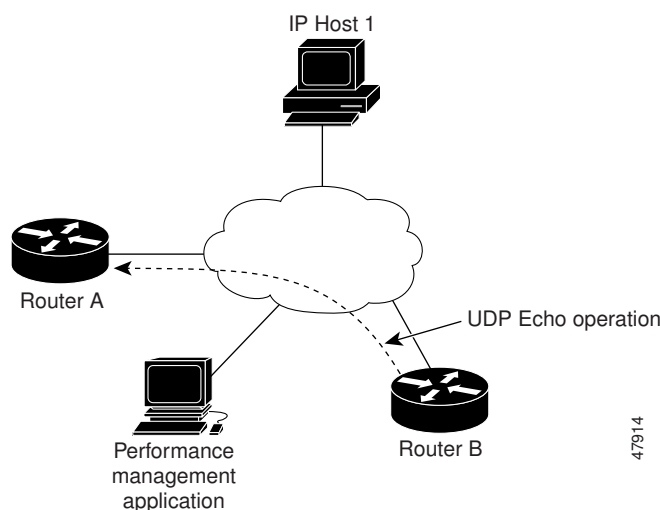
- [UDP Echo Operation, page 80](#)

UDP Echo Operation

The UDP echo operation measures end-to-end response time between a Cisco router 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 Router A has been configured as an IP SLAs Responder and Router B is configured as the source IP SLAs device.

Figure 9



Response time (round-trip time) is computed by measuring the time taken between sending a UDP echo request message from Router B to the destination router--Router A--and receiving a UDP echo reply from Router A. UDP echo accuracy is enhanced by using the IP SLAs Responder at Router A, the destination Cisco router. If the destination router is a Cisco router, 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 the Destination Device, page 80](#)
- [Configuring a UDP Echo Operation on the Source Device, page 82](#)
- [Scheduling IP SLAs Operations, page 88](#)

Configuring the IP SLAs Responder on the Destination Device

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 udp-echo ipaddress *ip-address* port *port***
4. **exit**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> • ip sla responder • ip sla responder udp-echo ipaddress <i>ip-address</i> port <i>port</i> Example: <pre>Router(config)# ip sla responder</pre> Example: <pre>Router(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000</pre>	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. or (Optional) Required only if protocol control is disabled on source. Permanently enables IP SLAs Responder functionality on specified IP address and port. <ul style="list-style-type: none"> • Control is enabled by default.
Step 4 exit Example: <pre>Router(config)# exit</pre>	(Optional) 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, page 82](#)
- [Configuring a UDP Echo Operation with Optional Parameters on the Source Device, page 83](#)

Configuring a Basic UDP Echo Operation on the Source Device

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. **frequency** *seconds*
6. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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.

Command or Action	Purpose
Step 4 udp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } <i>destination-port</i> [source-ip { <i>ip-address</i> <i>hostname</i> } source-port <i>port-number</i>] [control { enable disable }] Example: Router(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5 frequency <i>seconds</i> Example: Router(config-ip-sla-udp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6 end Example: Router(config-ip-sla-udp)# end	Returns to privileged EXEC mode.

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

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.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	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	udp-echo {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}] Example: Router(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	history buckets-kept size Example: Router(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: Router(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: Router(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.
Step 8	history enhanced [interval seconds] [buckets number-of-buckets] Example: Router(config-ip-sla-udp)# 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: <pre>Router(config-ip-sla-udp)# history filter failures</pre>	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	frequency <i>seconds</i> Example: <pre>Router(config-ip-sla-udp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	history hours-of-statistics-kept <i>hours</i> Example: <pre>Router(config-ip-sla-udp)# history hours-of-statistics-kept 4</pre>	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 12	history lives-kept <i>lives</i> Example: <pre>Router(config-ip-sla-udp)# history lives-kept 5</pre>	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	owner <i>owner-id</i> Example: <pre>Router(config-ip-sla-udp)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	request-data-size <i>bytes</i> Example: <pre>Router(config-ip-sla-udp)# request-data-size 64</pre>	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	history statistics-distribution-interval <i>milliseconds</i> Example: <pre>Router(config-ip-sla-udp)# history statistics-distribution-interval 10</pre>	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.

	Command or Action	Purpose
Step 16	tag <i>text</i> Example: Router(config-ip-sla-udp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	threshold <i>milliseconds</i> Example: Router(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 <i>milliseconds</i> Example: Router(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: <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> Example: Router(config-ip-sla-jitter)# tos 160 Example: Router(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 <i>number</i> Example: Router(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: Router(config-ip-sla-udp)# verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.

Command or Action	Purpose
Step 22 <code>exit</code> Example: <code>Router(config-ip-sla-udp)# exit</code>	Exits UDP configuration submode and returns to global configuration mode.

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 a multioperation group must 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. Do one of the following:
 - **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 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> • ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] • ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm:ss</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 6 show ip sla configuration Example: <pre>Router# show ip sla configuration</pre>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs UDP Echo Operations

- [Example Configuring a UDP Echo Operation, page 90](#)

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	<i>Cisco IOS IP SLAs Command Reference</i>

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 862	Echo 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 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 6 **Feature Information for the IP SLAs UDP Echo Operation**

Feature Name	Releases	Feature Information
IP SLAs UDP Jitter Operation	12.2(31)SB2	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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SRC	Support was added for operability in IPv6 networks.
	12.2(33)SB	
	12.4(20)T	
	Cisco IOS XE 3.1.0SG	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 93](#)
- [Restrictions for IP SLAs HTTP Operations, page 93](#)
- [Information About IP SLAs HTTP Operations, page 93](#)
- [How to Configure IP SLAs HTTP Operations, page 94](#)
- [Configuration Examples for IP SLAs HTTP Operations, page 103](#)
- [Additional References, page 105](#)
- [Feature Information for IP SLAs HTTP Operations, page 106](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 94](#)

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 lookup--RTT 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.

How to Configure IP SLAs HTTP Operations

- [Configuring an HTTP GET Operation on the Source Device, page 94](#)
- [Configuring an HTTP RAW Operation on the Source Device, page 99](#)
- [Scheduling IP SLAs Operations, page 88](#)

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, page 94](#)
- [Configuring an HTTP GET Operation with Optional Parameters on the Source Device, page 96](#)

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip sla <i>operation-number</i> Example: Router(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 <i>ip-address</i>] [version <i>version-number</i>] [source-ip {<i>ip-address</i> <i>hostname</i>}] [source-port <i>port-number</i>] [cache {enable disable}] [proxy <i>proxy-url</i>] Example: Router(config-ip-sla)# http get http://198.133.219.25	Defines an HTTP operation and enters IP SLA configuration mode.
Step 5 frequency <i>seconds</i> Example: Router(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 <code>end</code> Example: <code>Router(config-ip-sla-http)# end</code>	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 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. `http-raw-request`
12. `history lives-kept lives`
13. `owner owner-id`
14. `history statistics-distribution-interval milliseconds`
15. `tag text`
16. `threshold milliseconds`
17. `timeout milliseconds`
18. `tos number`
19. `end`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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	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: Router(config-ip-sla)# http get http://198.133.219.25	Defines an HTTP operation and enters IP SLA configuration mode.
Step 5	history buckets-kept size Example: Router(config-ip-sla-http)# 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-http)# 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-http)# 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-http)# 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-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 10	history hours-of-statistics-kept hours Example: Router(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 11	http-raw-request Example: Router(config-ip-sla-http)# http-raw-request	(Optional) Explicitly specifies the options for a GET request for an IP SLAs HTTP operation.
Step 12	history lives-kept lives Example: Router(config-ip-sla-http)# 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: Router(config-ip-sla-http)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	history statistics-distribution-interval milliseconds Example: Router(config-ip-sla-http)# 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 15	tag <i>text</i> Example: Router(config-ip-sla-http)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 16	threshold <i>milliseconds</i> Example: Router(config-ip-sla-http)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 17	timeout <i>milliseconds</i> Example: Router(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 18	tos <i>number</i> Example: Router(config-ip-sla-http)# tos 160	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 19	end Example: Router(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 Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip sla <i>operation-number</i> Example: Router(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 <i>ip-address</i>] [version <i>version-number</i>] [source-ip {<i>ip-address</i> <i>hostname</i>}] [source-port <i>port-number</i>] [cache {enable disable}] [proxy <i>proxy-url</i>] Example: Router(config-ip-sla)# http raw http://198.133.219.25	Defines an HTTP operation.
Step 5 http-raw-request Example: Router(config-ip-sla)# http-raw-request	Enters HTTP RAW configuration mode.

	Command or Action	Purpose
Step 6	Enter the required HTTP 1.0 command syntax. Example: Router(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: Router(config-ip-sla-http)# end	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.

Command or Action	Purpose
Step 6 <code>show ip sla configuration</code> Example: Router# <code>show ip sla configuration</code>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

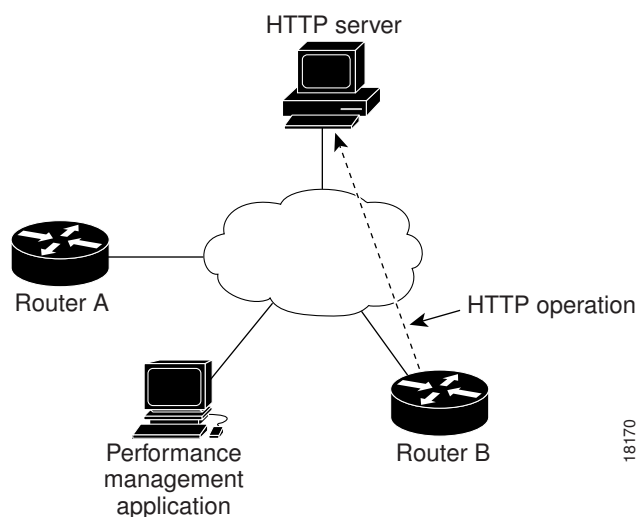
Configuration Examples for IP SLAs HTTP Operations

- [Example Configuring an HTTP GET Operation, page 104](#)
- [Example Configuring an HTTP RAW Operation, page 104](#)
- [Example Configuring an HTTP RAW Operation Through a Proxy Server, page 104](#)
- [Example Configuring an HTTP RAW Operation with Authentication, page 105](#)

Example Configuring an HTTP GET Operation

The following example shows 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



Router 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\nend\nip 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\n  http raw url http://site-test.cisco.com\n  http-raw-request\n  GET /lab/index.html HTTP/1.0\r\n  Authorization: Basic btNpdGT4biNvoZe=\r\n  \r\nend\nip 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	<i>Cisco IOS IP SLAs Command Reference</i>
Cisco IOS IP SLAs: general information	Cisco IOS IP SLAs Overview chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> .

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 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 7 *Feature Information for IP SLAs HTTP Operations*

Feature Name	Releases	Feature Information
IP SLAs HTTP Operation	12.2(31)SB2	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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party

trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 109](#)
- [Information About the IP SLAs TCP Connect Operation, page 109](#)
- [How to Configure the IP SLAs TCP Connect Operation, page 110](#)
- [Configuration Examples for IP SLAs TCP Connect Operations, page 120](#)
- [Additional References, page 121](#)
- [Feature Information for the IP SLAs TCP Connect Operation, page 122](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

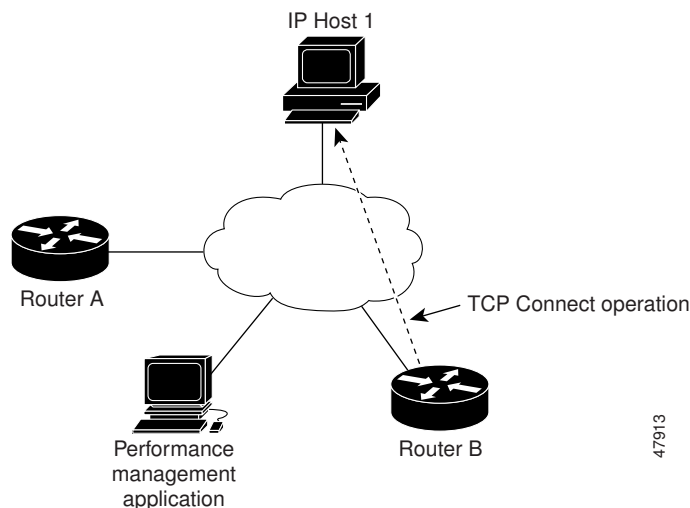
- [TCP Connect Operation, page 109](#)

TCP Connect Operation

The IP SLAs TCP Connect operation measures the response time taken to perform a TCP Connect operation between a Cisco router 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 Router 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



Connection response time is computed by measuring the time taken between sending a TCP request message from Router 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 router is a Cisco router, 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, page 110](#)
- [Configuring and Scheduling a TCP Connect Operation on the Source Device, page 112](#)

Configuring the IP SLAs Responder on the Destination Device

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> • ip sla responder • ip sla responder tcp-connect ipaddress <i>ip-address</i> port <i>port</i> Example: <pre>Router(config)# ip sla responder</pre> Example: <pre>Router(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000</pre>	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. or (Optional) Required only if protocol control is disabled on source. Permanently enables IP SLAs Responder functionality on specified IP address and port. <ul style="list-style-type: none"> • Control is enabled by default.
Step 4 exit Example: <pre>Router(config)# exit</pre>	(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](#), page 112
- [Configuring and Scheduling a Basic TCP Connect Operation on the Source Device](#), page 112
- [Configuring and Scheduling a TCP Connect Operation with Optional Parameters on the Source Device](#), page 114

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 and Scheduling 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. **exit**
7. **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**]
8. **exit**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>ip sla operation-number</code> Example: <pre>Router(config)# ip sla 10</pre>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4 <code>tcp-connect {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}]</code> Example: <pre>Router(config-ip-sla)# tcp-connect 172.29.139.132 5000</pre>	Defines a TCP Connect operation and enters IP SLA TCP configuration mode. <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5 <code>frequency seconds</code> Example: <pre>Router(config-ip-sla-tcp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6 <code>exit</code> Example: <pre>Router(config-ip-sla-tcp)# exit</pre>	Exits IP SLA TCP configuration mode and returns to global configuration mode.
Step 7 <code>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]</code> Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre>	Configures the scheduling parameters for an individual IP SLAs operation.
Step 8 <code>exit</code> Example: <pre>Router(config)# exit</pre>	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Example

The following example shows the configuration of an IP SLAs operation type of TCP Connect that will start immediately and run indefinitely.

```
ip sla 9
```

```
tcp-connect 172.29.139.132 5000
frequency 10
!
ip sla schedule 9 life forever start-time now
```

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuring and Scheduling 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. **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**]
21. **exit**
22. **show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	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	tcp-connect {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source- port port-number] [control {enable disable}] Example: Router(config-ip-sla)# tcp-connect 172.29.139.132 5000	Defines a TCP Connect operation and enters IP SLA TCP configuration mode. <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	history buckets-kept size Example: Router(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: Router(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: Router(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: Router(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 <i>seconds</i> Example: Router(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 <i>hours</i> Example: Router(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 <i>lives</i> Example: Router(config-ip-sla-tcp)# history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Router(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 <i>milliseconds</i> Example: Router(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 <i>text</i> Example: Router(config-ip-sla-tcp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	threshold <i>milliseconds</i> Example: Router(config-ip-sla-tcp)# 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 <code>timeout</code> <i>milliseconds</i> Example: <pre>Router(config-ip-sla-tcp)# timeout 10000</pre>	(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: <ul style="list-style-type: none"> • <code>tos</code> <i>number</i> • <code>traffic-class</code> <i>number</i> Example: <pre>Router(config-ip-sla-jitter)# tos 160</pre> Example: <pre>Router(config-ip-sla-jitter)# traffic-class 160</pre>	(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 18 <code>flow-label</code> <i>number</i> Example: <pre>Router(config-ip-sla-tcp)# flow-label 112233</pre>	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 19 <code>exit</code> Example: <pre>Router(config-ip-sla-tcp)# exit</pre>	Exits TCP configuration submode and returns to global configuration mode.
Step 20 <code>ip sla schedule</code> <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i> [<i>ageout seconds</i>] [recurring]} Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre>	Configures the scheduling parameters for an individual IP SLAs operation.
Step 21 <code>exit</code> Example: <pre>Router(config)# exit</pre>	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Command or Action	Purpose
Step 22 <code>show ip sla configuration [operation-number]</code> Example: Router# <code>show ip sla configuration 10</code>	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Example

The following sample output shows the configuration of all the IP SLAs parameters (including defaults) for the TCP Connect operation number 9.

```
Router# show ip sla configuration 9
Complete Configuration Table (includes defaults)
Entry Number: 9
Owner:
Tag: SL-SGU
Type of Operation to Perform: tcpConnect
Reaction and History Threshold (milliseconds): 5000
Operation Frequency (seconds): 20
Operation Timeout (milliseconds): 60000
Verify Data: FALSE
Status of Entry (SNMP RowStatus): active
Protocol Type: ipTcpConn
Target Address: 172.29.139.132
Source Address: 0.0.0.0
Target Port: 5000
Source Port: 0
Request Size (ARR data portion): 1
Response Size (ARR data portion): 1
Control Packets: enabled
Loose Source Routing: disabled
LSR Path:
Type of Service Parameters: 128
Life (seconds): infinite - runs forever
Next Scheduled Start Time: Start Time already passed
Entry Ageout (seconds): never
Connection Loss Reaction Enabled: FALSE
Timeout Reaction Enabled: FALSE
Threshold Reaction Type: never
Threshold Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Reaction Type: none
Verify Error Reaction Enabled: FALSE
Number of Statistic Hours kept: 2
Number of Statistic Paths kept: 1
Number of Statistic Hops kept: 1
Number of Statistic Distribution Buckets kept: 1
Statistic Distribution Interval (milliseconds): 20
Number of History Lives kept: 0
Number of History Buckets kept: 15
Number of History Samples kept: 1
History Filter Type: none
```

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data

verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.

- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs TCP Connect Operations

- [Example Configuring a TCP Connect Operation, page 120](#)

Example Configuring a TCP Connect Operation

The following example shows how to configure a TCP Connect operation from Router 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 source (Router 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 router and a well-known TCP port is used, there is no need to send the control message.

Router A Configuration

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

Router B 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	<i>Cisco IOS IP SLAs Command Reference</i>

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 8 *Feature Information for the IP SLAs TCP Connect Operation*

Feature Name	Releases	Feature Information
IP SLAs TCP Connect Operation	12.2(31)SB2	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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SRC	Support was added for operability in IPv6 networks.
	12.2(33)SB	
	12.4(20)T	
	Cisco IOS XE 3.1.0SG	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 123](#)
- [Restrictions for IP SLAs ICMP Echo Operations, page 123](#)
- [Information About IP SLAs ICMP Echo Operations, page 123](#)
- [How to Configure IP SLAs ICMP Echo Operations, page 124](#)
- [Configuration Examples for IP SLAs ICMP Echo Operations, page 132](#)
- [Additional References, page 133](#)
- [Feature Information for IP SLAs ICMP Echo Operations, page 134](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

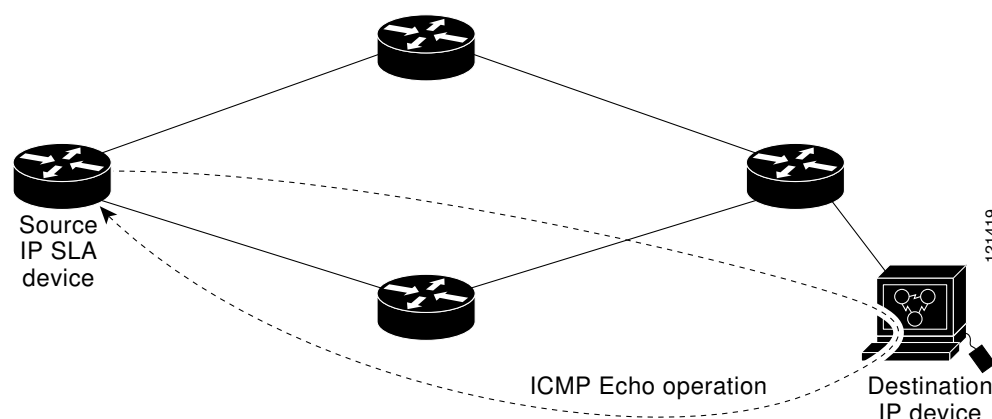
- [ICMP Echo Operation, page 124](#)

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



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, page 124](#)
- [Scheduling IP SLAs Operations, page 88](#)

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, page 124](#)
- [Configuring an ICMP Echo Operation with Optional Parameters, page 126](#)

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip sla <i>operation-number</i> Example: Router(config)# ip sla 6	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4 icmp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> } source-interface <i>interface-name</i>] Example: Router(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 <i>seconds</i> Example: Router(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: Router(config-ip-sla-echo)# end	Exits to privileged EXEC mode.

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. **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. Do one of the following:
 - **tos** *number*
 - **traffic-class** *number*
19. **flow-label** *number*
20. **verify-data**
21. **vrf** *vrf-name*
22. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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 6	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	icmp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> } source-interface <i>interface-name</i>] Example: Router(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	history buckets-kept <i>size</i> Example: Router(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 6	history distributions-of-statistics-kept <i>size</i> Example: Router(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.

	Command or Action	Purpose
Step 7	history enhanced [<i>interval seconds</i>] [<i>buckets number-of-buckets</i>] Example: <pre>Router(config-ip-sla-echo)# history enhanced interval 900 buckets 100</pre>	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter { none all overThreshold failures } Example: <pre>Router(config-ip-sla-echo)# history filter failures</pre>	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	frequency <i>seconds</i> Example: <pre>Router(config-ip-sla-echo)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	history hours-of-statistics-kept <i>hours</i> Example: <pre>Router(config-ip-sla-echo)# history hours-of- statistics-kept 4</pre>	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	history lives-kept <i>lives</i> Example: <pre>Router(config-ip-sla-echo)# history lives-kept 5</pre>	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: <pre>Router(config-ip-sla-echo)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	request-data-size <i>bytes</i> Example: <pre>Router(config-ip-sla-echo)# request-data-size 64</pre>	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.

	Command or Action	Purpose
Step 14	history statistics-distribution-interval <i>milliseconds</i> Example: <pre>Router(config-ip-sla-echo)# history statistics-distribution-interval 10</pre>	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 15	tag <i>text</i> Example: <pre>Router(config-ip-sla-echo)# tag TelnetPollServer1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 16	threshold <i>milliseconds</i> Example: <pre>Router(config-ip-sla-echo)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 17	timeout <i>milliseconds</i> Example: <pre>Router(config-ip-sla-echo)# timeout 10000</pre>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 18	Do one of the following: <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> Example: <pre>Router(config-ip-sla-jitter)# tos 160</pre> Example: <pre>Router(config-ip-sla-jitter)# traffic-class 160</pre>	(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 19	flow-label <i>number</i> Example: <pre>Router(config-ip-sla-echo)# flow-label 112233</pre>	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.

Command or Action	Purpose
Step 20 <code>verify-data</code> Example: <code>Router(config-ip-sla-echo)# verify-data</code>	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 21 <code>vrf vrf-name</code> Example: <code>Router(config-ip-sla-echo)# vrf vpn-A</code>	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 22 <code>end</code> Example: <code>Router(config-ip-sla-echo)# end</code>	Exits to privileged EXEC mode.

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 a multioperation group must 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. Do one of the following:
 - **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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> • ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] • ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.

Command or Action	Purpose
Step 6 <code>show ip sla configuration</code> Example: Router# <code>show ip sla configuration</code>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs ICMP Echo Operations

- [Example Configuring an ICMP Echo Operation, page 132](#)

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

Related Documents

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

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 862	Echo 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 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 9 *Feature Information for IP SLAs ICMP Echo Operations*

Feature Name	Releases	Feature Information
IP SLAs ICMP Echo Operation	12.2(31)SB2	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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SB	Support was added for operability in IPv6 networks.
	12.2(33)SRC	
	12.4(20)T	
	Cisco IOS XE 3.1.0SG	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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 router and 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, page 135](#)
- [Restrictions for IP SLAs ICMP Path Echo Operations, page 135](#)
- [Information About IP SLAs ICMP Path Echo Operations, page 135](#)
- [How to Configure IP SLAs ICMP Path Echo Operations, page 136](#)
- [Configuration Examples for IP SLAs ICMP Path Echo Operations, page 145](#)
- [Additional References, page 146](#)
- [Feature Information for IP SLAs ICMP Path Echo Operations, page 147](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 136](#)

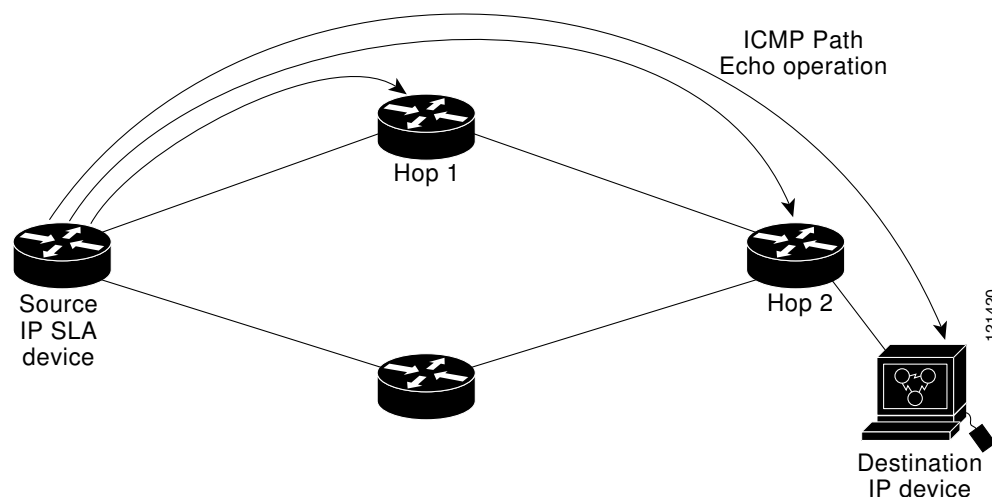
ICMP Path Echo Operation

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 router and 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 router 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



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, page 136](#)
- [Scheduling IP SLAs Operations, page 88](#)

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, page 137](#)
- [Configuring an ICMP Path Echo Operation with Optional Parameters on the Source Device, page 138](#)

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-id</i> Example: Router(config)# ip sla 7	Specifies an ID number for the operation being configured, and enters IP SLA configuration mode.
Step 4	path-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> }] Example: Router(config-ip-sla)# path-echo protocol 172.29.139.134	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.

Command or Action	Purpose
Step 5 <code>frequency seconds</code> Example: <code>Router(config-ip-sla-pathEcho)# frequency 30</code>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6 <code>end</code> Example: <code>Router(config-ip-sla-pathEcho)# end</code>	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 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. **paths-of-statistics-kept** *size*
14. **request-data-size** *bytes*
15. **samples-of-history-kept** *samples*
16. **history statistics-distribution-interval** *milliseconds*
17. **tag** *text*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **tos** *number*
21. **verify-data**
22. **vrf** *vrf-name*
23. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<code>ip sla operation-number</code> Example: <pre>Router(config)# ip sla 10</pre>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	<code>path-echo {destination-ip-address destination-hostname} [source-ip {ip-address hostname}]</code> Example: <pre>Router(config-ip-sla)# path-echo 172.29.139.134</pre>	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.
Step 5	<code>history buckets-kept size</code> Example: <pre>Router(config-ip-sla-pathEcho)# history buckets-kept 25</pre>	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	<code>history distributions-of-statistics-kept size</code> Example: <pre>Router(config-ip-sla-pathEcho)# history distributions-of-statistics-kept 5</pre>	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	<code>history enhanced [interval seconds] [buckets number-of-buckets]</code> Example: <pre>Router(config-ip-sla-pathEcho)# history enhanced interval 900 buckets 100</pre>	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	<code>history filter {none all overThreshold failures}</code> Example: <pre>Router(config-ip-sla-pathEcho)# history filter failures</pre>	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	<code>frequency seconds</code> Example: <pre>Router(config-ip-sla-pathEcho)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 10	history hours-of-statistics-kept <i>hours</i> Example: Router(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.
Step 11	history lives-kept <i>lives</i> Example: Router(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 12	owner <i>owner-id</i> Example: Router(config-ip-sla-pathEcho)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	paths-of-statistics-kept <i>size</i> Example: Router(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 14	request-data-size <i>bytes</i> Example: Router(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 15	samples-of-history-kept <i>samples</i> Example: Router(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 16	history statistics-distribution-interval <i>milliseconds</i> Example: Router(config-ip-sla-pathEcho)# 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 17 <code>tag text</code> Example: <pre>Router(config-ip-sla-pathEcho)# tag TelnetPollServer1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18 <code>threshold milliseconds</code> Example: <pre>Router(config-ip-sla-pathEcho)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 19 <code>timeout milliseconds</code> Example: <pre>Router(config-ip-sla-pathEcho)# timeout 10000</pre>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 20 <code>tos number</code> Example: <pre>Router(config-ip-sla-pathEcho)# tos 160</pre>	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 21 <code>verify-data</code> Example: <pre>Router(config-ip-sla-pathEcho)# verify-data</pre>	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22 <code>vrf vrf-name</code> Example: <pre>Router(config-ip-sla-pathEcho)# vrf vpn-A</pre>	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 23 <code>end</code> Example: <pre>Router(config-ip-sla-pathEcho)# end</pre>	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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	Enables privileged EXEC mode.
	Example: <pre>Router> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: <pre>Router# configure terminal</pre>	

Command or Action	Purpose
<p>Step 3 Do one of the following:</p> <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] <p>Example:</p> <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> <p>Example:</p> <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	<p>For individual IP SLAs operations only:</p> <p>Configures the scheduling parameters for an individual IP SLAs operation.</p> <p>or</p> <p>For multioperation scheduler only:</p> <p>Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.</p>
<p>Step 4 exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits to privileged EXEC mode.</p>
<p>Step 5 show ip sla group schedule</p> <p>Example:</p> <pre>Router# show ip sla group schedule</pre>	<p>(Optional) Displays the IP SLAs group schedule details.</p>
<p>Step 6 show ip sla configuration</p> <p>Example:</p> <pre>Router# show ip sla configuration</pre>	<p>(Optional) Displays the IP SLAs configuration details.</p>

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.

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

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.

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

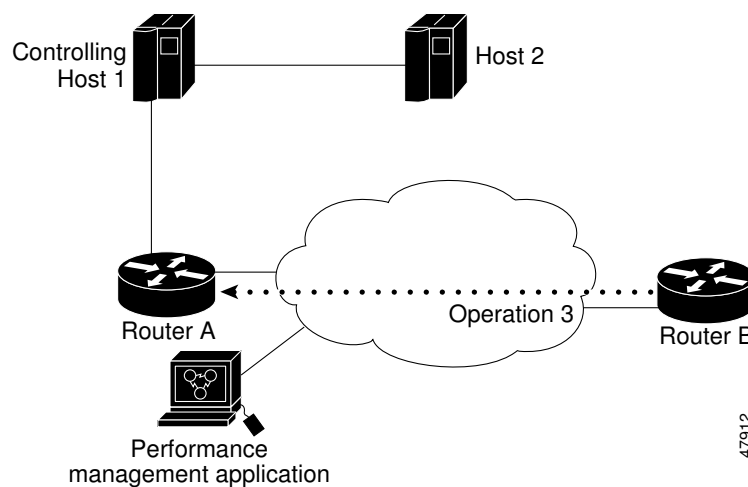
Configuration Examples for IP SLAs ICMP Path Echo Operations

- [Example Configuring an ICMP Path Echo Operation, page 145](#)

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



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

Router 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

Related Documents

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

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 862	Echo 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 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 10 Feature Information for IP SLAs ICMP Path Echo Operations

Feature Name	Releases	Feature Information
IP SLAs ICMP Path Echo Operation	12.2(31)SB2	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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 149](#)
- [Prerequisites for ICMP Path Jitter Operations, page 149](#)
- [Restrictions for ICMP Path Jitter Operations, page 150](#)
- [Information About IP SLAs ICMP Path Jitter Operations, page 150](#)
- [How to Configure the IP SLAs ICMP Path Jitter Operation, page 151](#)
- [Configuration Examples for IP SLAs ICMP Path Jitter Operations, page 158](#)
- [Additional References, page 159](#)
- [Feature Information for IP SLAs ICMP Path Jitter Operations, page 160](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- The IP SLAs ICMP Path Jitter operation 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, use of the IP SLAs UDP Jitter operation is recommended.
- The jitter values obtained using the ICMP Path Jitter operation are approximates because ICMP does not provide the capability to embed processing times on routers in the packet. If the target router does not place ICMP packets as the highest priority, then the router will not respond properly. ICMP performance also can be affected by the configuration of priority queueing on the router and by ping response.
- The 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.
- The IP SLAs Path Jitter operation 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, page 150](#)

ICMP Path Jitter Operation

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

The ICMP Path Jitter operation can be used a supplement to the standard UDP Jitter operation. For example, results from the UDP Jitter operation may indicate unexpected delays or high jitter values; the 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 the ICMP Path Jitter operation are approximates because ICMP only provides round trip times.

The ICMP Path Jitter operation functions 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, page 151](#)
- [Configuring an ICMP Path Jitter Operation on the Source Device, page 152](#)
- [Scheduling IP SLAs Operations, page 88](#)

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.

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip sla responder Example: Example: Router(config)# ip sla responder	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. <ul style="list-style-type: none"> Control is enabled by default.
Step 4 exit Example: Router(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, page 152](#)
- [Configuring an ICMP Path Jitter Operation with Additional Parameters, page 154](#)

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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	path-jitter { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> }] [num-packets <i>packet-number</i>] [interval <i>milliseconds</i>] [targetOnly] Example: Router(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22	Defines an ICMP Path Jitter operation and enters IP SLA Path Jitter configuration mode.
Step 5	frequency <i>seconds</i> Example: Router(config-ip-sla-pathJitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

Command or Action	Purpose
Step 6 <code>end</code> Example: <code>Router(config-ip-sla-pathJitter)# end</code>	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.

```
Router(config)# ip sla 1
Router(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 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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	path-jitter {destination-ip-address destination-hostname} [source-ip {ip-address hostname}] [num-packets packet-number] [interval milliseconds] [targetOnly] Example: Router(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22	Defines an ICMP Path Jitter operation and enters IP SLA Path Jitter configuration mode.
Step 5	frequency seconds Example: Router(config-ip-sla-pathJitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	owner owner-id Example: Router(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: Router(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: Router(config-ip-sla-pathJitter)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 9	timeout <i>milliseconds</i> Example: Router(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 <i>vrf-name</i> Example: Router(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: Router(config-ip-sla-pathJitter)# end	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.

Command or Action	Purpose
Step 6 <code>show ip sla configuration</code> Example: Router# <code>show ip sla configuration</code>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs ICMP Path Jitter Operations

- [Example Configuring a Path Jitter Operation, page 158](#)

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.

```
Router# configure terminal
Router(config)# ip sla 15011
Router(config-sla-monitor)# path-jitter 10.222.1.100 source-ip 10.222.3.100 num-packets 20
Router(config-sla-monitor-pathJitter)# frequency 30
Router(config-sla-monitor-pathJitter)# exit
Router(config)# ip sla schedule 15011 life forever start-time now
```

```

Router(config)# exit
Router# 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	<i>Cisco IOS IP SLAs Command Reference</i>
Cisco IOS IP SLAs: general information	Cisco IOS IP SLAs Overview chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> .

Standards

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

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

RFCs

RFCs	Title
RFC 1889 ¹	<i>RTP: A Transport Protocol for Real-Time Applications</i> ; see the section “Estimating the Interarrival Jitter”

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 11 Feature Information for IP SLAs ICMP Path Jitter Operations

Feature Name	Releases	Feature Information
IP SLAs Path Jitter 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 Internet Control Message Protocol (ICMP) path jitter operation allows you to measure hop-by-hop jitter (inter-packet delay variance).

¹ Support for the listed RFC is not claimed; listed as a reference only.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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 a 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, page 163](#)
- [Restrictions for IP SLAs FTP Operations, page 163](#)
- [Information About IP SLAs FTP Operations, page 163](#)
- [How to Configure IP SLAs FTP Operations, page 164](#)
- [Configuration Examples for IP SLAs FTP Operations, page 171](#)
- [Additional References, page 172](#)
- [Feature Information for IP SLAs FTP Operations, page 173](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

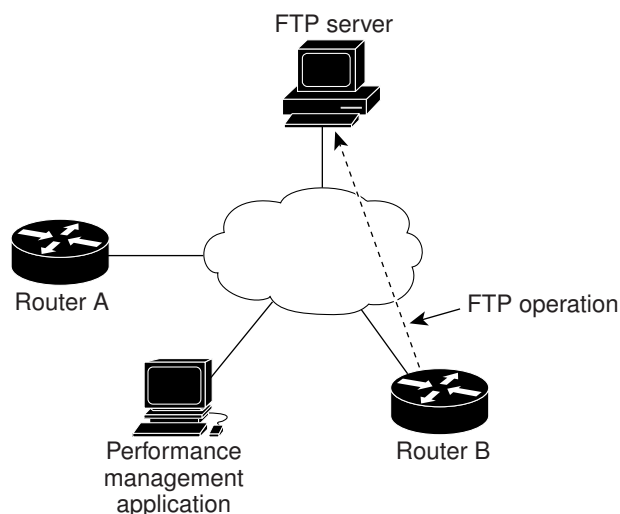
- [FTP Operation, page 164](#)

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 Router 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



38175

Connection response time is computed by measuring the time taken to download a file to Router 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, page 165](#)
- [Scheduling IP SLAs Operations, page 88](#)

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, page 165](#)
- [Configuring an FTP Operation with Optional Parameters on the Source Device, page 166](#)

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip sla <i>operation-number</i> Example: Router(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

Command or Action	Purpose
Step 4 <code>ftp get url [source-ip {ip-address hostname}] [mode {passive active}]</code> Example: <pre>Router(config-ip-sla)# ftp get ftp:// username:password@hostip/test.cap</pre>	Defines an FTP operation and enters IP SLA FTP configuration mode.
Step 5 <code>frequency seconds</code> Example: <pre>Router(config-ip-sla-ftp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6 <code>end</code> Example: <pre>Router(config-ip-sla-ftp)# exit</pre>	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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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	ftp get url [source-ip {ip-address hostname}] [mode {passive active}] Example: Router(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: Router(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: Router(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: Router(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: Router(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: Router(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: Router(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: Router(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: Router(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: Router(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: Router(config-ip-sla-ftp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 15	threshold <i>milliseconds</i> Example: Router(config-ip-sla-ftp)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	timeout <i>milliseconds</i> Example: Router(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: Router(config-ip-sla-ftp)# end	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.

Command or Action	Purpose
Step 6 <code>show ip sla configuration</code> Example: Router# <code>show ip sla configuration</code>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs FTP Operations

- [Example Configuring an FTP Operation, page 171](#)

Example Configuring an FTP Operation

The following example shows how to configure an FTP operation from Router 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.

Router 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
Cisco IOS IP SLAs commands	<i>Cisco IOS IP SLAs Command Reference</i>
Cisco IOS IP SLAs: general information	Cisco IOS IP SLAs Overview chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> .

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 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 12 Feature Information for IP SLAs FTP Operations

Feature Name	Releases	Feature Information
IP SLAs FTP Operation	12.2(31)SB2	The Cisco IOS 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.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 175](#)
- [Information About IP SLAs DNS Operations, page 175](#)
- [How to Configure IP SLAs DNS Operations, page 176](#)
- [Configuration Examples for IP SLAs DNS Operations, page 183](#)
- [Additional References, page 184](#)
- [Feature Information for IP SLAs DNS Operations, page 185](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

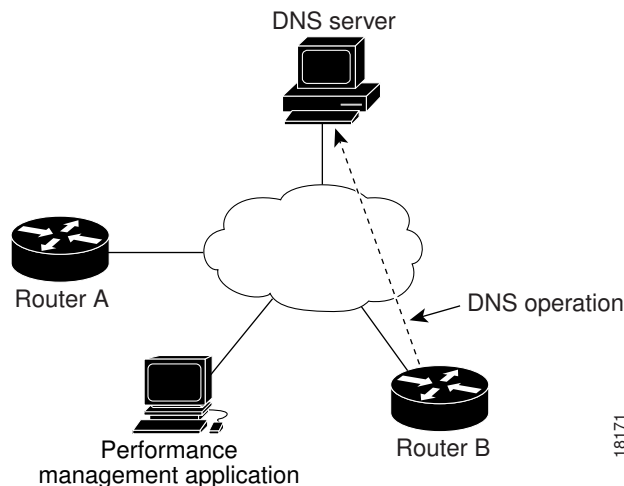
- [DNS Operation, page 175](#)

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 Router 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



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 Router 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, page 176](#)
- [Scheduling IP SLAs Operations, page 88](#)

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, page 176](#)
- [Configuring a DNS Operation with Optional Parameters on the Source Device, page 178](#)

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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	dns { <i>destination-ip-address</i> <i>destination-hostname</i> } name-server <i>ip-address</i> [source-ip { <i>ip-address</i> <i>hostname</i> } source-port <i>port-number</i>] Example: Router(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: Router(config-ip-sla-dns)# frequency 60	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

Command or Action	Purpose
Step 6 <code>end</code> Example: <code>Router(config-ip-sla-dns)# end</code>	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 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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	dns {destination-ip-address destination-hostname} name-server ip-address [source-ip {ip-address hostname} source-port port-number] Example: Router(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: Router(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: Router(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: Router(config-ip-sla-dns)# 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-dns)# 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-dns)# 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-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: Router(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: Router(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: Router(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: Router(config-ip-sla-dns)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 15	threshold <i>milliseconds</i> Example: Router(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 <i>milliseconds</i> Example: Router(config-ip-sla-dns)# 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-dns)# end	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.

Command or Action	Purpose
Step 6 <code>show ip sla configuration</code> Example: Router# <code>show ip sla configuration</code>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs DNS Operations

- [Example Configuring a DNS Operation, page 183](#)

Example Configuring a DNS Operation

The following example shows how to configure a DNS operation from Router B to the DNS server (IP address 172.20.2.132) as shown in the "DNS Operation" figure in the "DNS peration" 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.

Router 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	<i>Cisco IOS IP SLAs Command Reference</i>
Cisco IOS IP SLAs: general information	Configuring IOS IP SLAs Overview chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i>

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 IP SLAs DNS 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 13 Feature Information for the IP SLAs DNS Operation

Feature Name	Releases	Feature Information
IP SLAs DNS Operation	12.2(31)SB2	The Cisco IOS IP SLAs Domain Name System (DNS) operation allows you to measure the difference between the time taken to send a DNS request and receive a reply.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



Configuring IP SLAs DHCP Operations

This module describes how to configure an IP Service Level Agreements (SLAs) Dynamic Host Control Protocol (DHCP) operation to measure the response time between a Cisco device and a DHCP server to obtain an IP address.

- [Finding Feature Information, page 187](#)
- [Information About IP SLAs DHCP Operations, page 187](#)
- [How to Configure IP SLAs DHCP Operations, page 188](#)
- [Configuration Examples for IP SLAs DHCP Operations, page 195](#)
- [Additional References, page 195](#)
- [Feature Information for IP SLAs DHCP Operations, page 196](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 187](#)
- [IP SLAs DHCP Relay Agent Options, page 188](#)

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 router. If a specific server is configured on the router, 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 router, 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.

The IP SLAs DHCP operation contains a relay agent information option--Option 82--which is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the relay agent information option may use the information to implement IP address or other parameter assignment policies. The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

Option 82 includes three suboptions that convey information known by the relay agent:

- **circuit-id** --identifies the incoming circuit.
- **remote-id** --provides a trusted identifier for a remote high-speed modem.
- **subnet-mask** --identifies the mask of the logical IP subnet from which the relay agent received the client DHCP packet.

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, page 188](#)
- [Scheduling IP SLAs Operations, page 88](#)

Configuring a DHCP Operation on the Source Device

Perform one of the following tasks:

- [Configuring a Basic DHCP Operation, page 188](#)
- [Configuring a DHCP Operation with Optional Parameters, page 189](#)

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*}] [**option-82** [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**subnet-mask** *subnet-mask*]]
5. **frequency** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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	dhcp { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> }] [option-82 [circuit-id <i>circuit-id</i>] [remote-id <i>remote-id</i>] [subnet-mask <i>subnet-mask</i>]] Example: Router(config-ip-sla)# dhcp 10.10.10.3	Defines a DHCP operation and enters IP SLA DHCP configuration mode.
Step 5	frequency seconds Example: Router(config-ip-sla-dhcp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Router(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* }] [**option-82** [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**subnet-mask** *subnet-mask*]]
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	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	ip sla <i>operation-number</i>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
	Example: Router(config)# ip sla 10	

	Command or Action	Purpose
Step 4	<p>dhcp {<i>destination-ip-address</i> <i>destination-hostname</i>} [source-ip {<i>ip-address</i> <i>hostname</i>}] [option-82 [circuit-id <i>circuit-id</i>] [remote-id <i>remote-id</i>] [subnet-mask <i>subnet-mask</i>]]</p> <p>Example:</p> <pre>Router(config-ip-sla)# dhcp 10.10.10.3 option-82 circuit-id 10005A6F1234</pre>	Defines a DHCP operation and enters IP SLA DHCP configuration mode.
Step 5	<p>history buckets-kept <i>size</i></p> <p>Example:</p> <pre>Router(config-ip-sla-dhcp)# history buckets-kept 25</pre>	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	<p>history distributions-of-statistics-kept <i>size</i></p> <p>Example:</p> <pre>Router(config-ip-sla-dhcp)# history distributions-of- statistics-kept 5</pre>	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	<p>history enhanced [interval <i>seconds</i>] [buckets <i>number-of-buckets</i>]</p> <p>Example:</p> <pre>Router(config-ip-sla-dhcp)# history enhanced interval 900 buckets 100</pre>	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	<p>history filter {none all overThreshold failures}</p> <p>Example:</p> <pre>Router(config-ip-sla-dhcp)# history filter failures</pre>	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	<p>frequency <i>seconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-dhcp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

Command or Action	Purpose
Step 10 history hours-of-statistics-kept <i>hours</i> Example: Router(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 11 history lives-kept <i>lives</i> Example: Router(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 12 owner <i>owner-id</i> Example: Router(config-ip-sla-dhcp)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13 history statistics-distribution-interval <i>milliseconds</i> Example: Router(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 14 tag <i>text</i> Example: Router(config-ip-sla-dhcp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15 threshold <i>milliseconds</i> Example: Router(config-ip-sla-dhcp)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16 timeout <i>milliseconds</i> Example: Router(config-ip-sla-dhcp)# 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 <code>end</code> Example: <code>Router(config-ip-sla-dhcp)# end</code>	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 6 show ip sla configuration Example: <pre>Router# show ip sla configuration</pre>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs DHCP Operations

- [Example Configuration for an IP SLAs DHCP Operation, page 195](#)

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.

Router B Configuration

```
ip dhcp-server 172.16.20.3
!
ip sla 12
  dhcp 10.10.10.3 option-82 circuit-id 10005A6F1234
  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

Related Topic	Document Title
Cisco IOS IP SLAs commands	<i>Cisco IOS IP SLAs Command Reference</i>
Cisco IOS IP SLAs: general information	Configuring IOS IP SLAs Overview chapter of the <i>Cisco IP SLAs Configuration Guide</i> .
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 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 14 **Feature Information for IP SLAs DHCP Operations**

Feature Name	Releases	Feature Information
IP SLAs DHCP Operation	12.2(31)SB2	The Cisco IOS IP SLAs Dynamic Host Control Protocol (DHCP) operation allows you to schedule and measure the network response time between a Cisco device and a DHCP server to obtain an IP address.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 199](#)
- [Prerequisites, page 199](#)
- [Information About IP SLAs DLSw+ Operations, page 199](#)
- [How to Configure IP SLAs DLSw+ Operations, page 200](#)
- [Configuration Examples for IP SLAs DLSw+ Operations, page 207](#)
- [Additional References, page 208](#)
- [Feature Information for Cisco IOS IP SLAs DLSw+ Operations, page 209](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 199](#)

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



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, page 200](#)
- [Scheduling IP SLAs Operations, page 88](#)

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, page 200](#)
- [Configuring an IP SLAs DLSw+ Operation with Optional Parameters on the Source Device, page 201](#)

Configuring a Basic DLSw+ Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **dls w 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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Router(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	dls w peer-ipaddr <i>ip-address</i> Example: Router(config-ip-sla)# dls w peer-ipaddr 172.21.27.11	Defines a DLSw+ operation and enters IP SLA DLSw+ configuration mode.
Step 5	frequency <i>seconds</i> Example: Router(config-ip-sla-dls w)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Router(config-ip-sla-dls w)# 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	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	ip sla <i>operation-number</i>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
	Example: Router(config)# ip sla 10	

	Command or Action	Purpose
Step 4	dlsw peer-ipaddr <i>ip-address</i> 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 <i>size</i> 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 <i>size</i> 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 [<i>interval seconds</i>] [<i>buckets number-of-buckets</i>] 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 { <i>none</i> <i>all</i> <i>overThreshold</i> <i>failures</i> } 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 <i>seconds</i> 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 <i>hours</i> 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 <i>lives</i> 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 <i>owner-id</i> 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 <i>bytes</i> 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 <i>milliseconds</i> 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 <i>text</i> Example: Router(config-ip-sla-dlsw)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 16 threshold <i>milliseconds</i> 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 <i>milliseconds</i> 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.

Command or Action	Purpose
Step 18 <code>end</code> Example: <code>Router(config-ip-sla-dlsw)# exit</code>	Exits to privileged EXEC mode.

Scheduling 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 must 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. Do one of the following:
 - **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 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 Do one of the following: <ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life{forever <i>seconds</i>}] [start-time{<i>hh:mm:ss</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] Example: <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.
Step 4 exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 6 show ip sla configuration Example: <pre>Router# show ip sla configuration</pre>	(Optional) Displays the IP SLAs configuration details.

- [Troubleshooting Tips, page 16](#)
- [What to Do Next, page 16](#)

Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debugipsla 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.

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

Configuration Examples for IP SLAs DLSw+ Operations

- [Example IP SLAs DLSw+ Operation Configuration, page 207](#)

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
Cisco IOS IP SLAs commands	<i>Cisco IOS IP SLAs Command Reference</i>
Cisco IOS IP SLAs: general information	Configuring IOS IP SLAs Overview chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> .

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 15 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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 211](#)
- [Prerequisites for an IP SLAs Multioperation Scheduler, page 211](#)
- [Information About an IP SLAs Multioperation Scheduler, page 211](#)
- [How to Configure an IP SLAs Multioperation Scheduler, page 218](#)
- [Configuration Examples for an IP SLAs Multioperation Scheduler, page 223](#)
- [Additional References, page 224](#)
- [Feature Information for a Cisco IOS IP SLAs Multioperation Scheduler, page 225](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 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, page 212](#)

- [IP SLAs Random Scheduler, page 218](#)

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, page 213](#)
- [IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency, page 214](#)
- [Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period, page 215](#)
- [IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency, page 216](#)

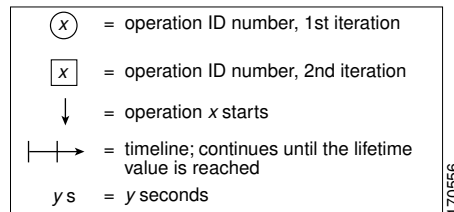
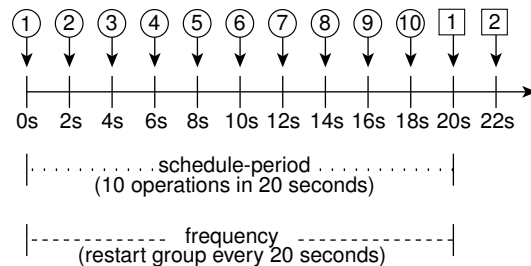
Default Behavior of IP SLAs Multiple Operations Scheduling

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 frequency is optional because 20 is the default.

Figure 18

ip sla group schedule 1 1-10 schedule-period 20 [frequency 20]



170556

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.

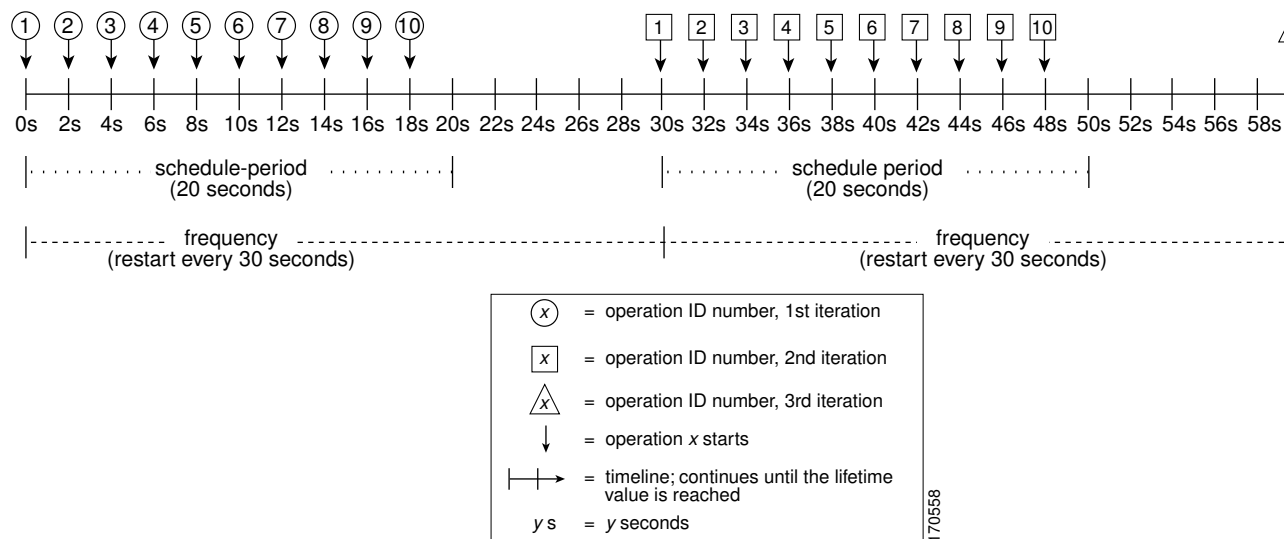
IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency

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

ip sla group schedule 2 1-10 schedule-period 20 frequency 30



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.

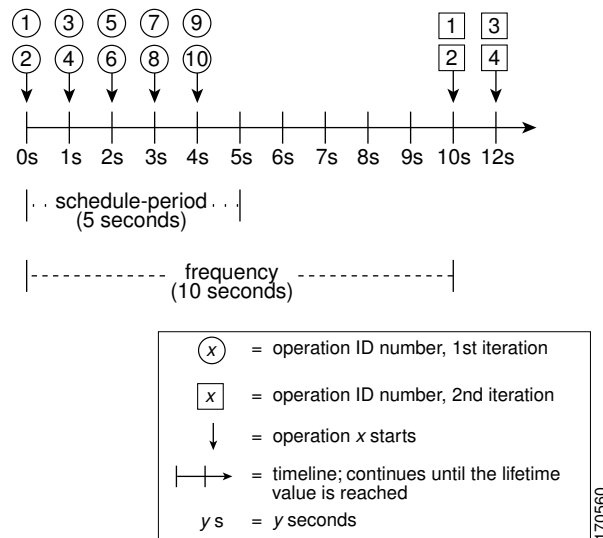
Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period

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

ip sla group schedule 3 1-10 schedule-period 5 frequency 10



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.

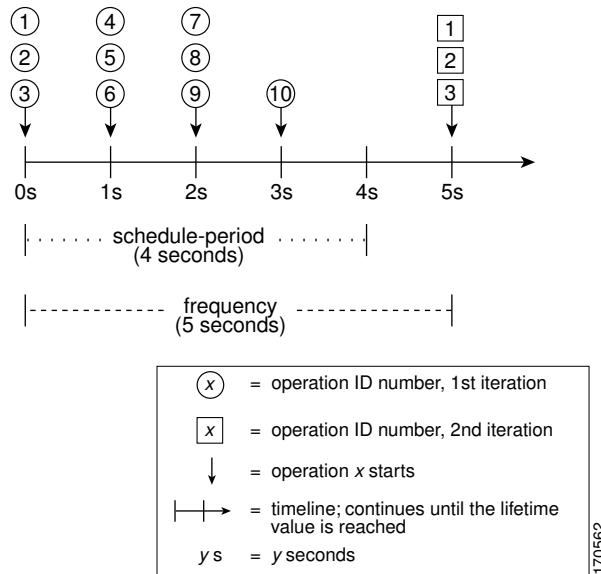
As the frequency is set to 10 in this example, each iteration of operation group 3 will start 10 seconds after the start of the previous iteration. However, this distribution is not optimal as there is a gap of 5 seconds (frequency minus schedule period) between the cycles.

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

ip sla group schedule 4 1-10 schedule-period 4 frequency 5



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.

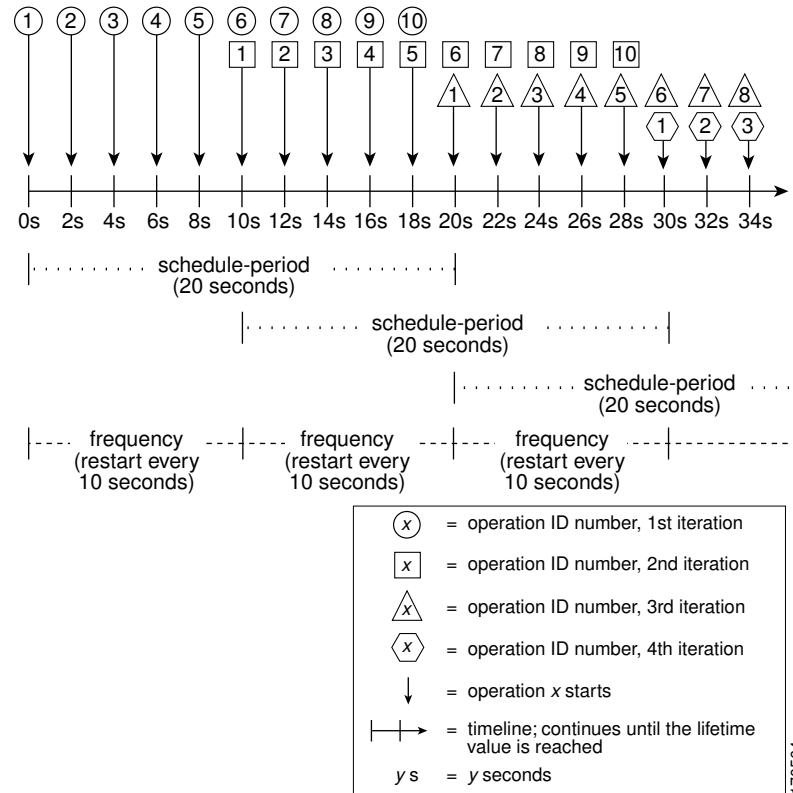
IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency

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 sla group schedule 5 1-10 schedule-period 20 frequency 10



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, page 219](#)
- [Enabling the IP SLAs Random Scheduler, page 220](#)
- [Verifying IP SLAs Multiple Operations Scheduling, page 221](#)

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 ip sla group schedule <i>group-operation-number operation-id-numbers schedule-period schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life { forever <i>seconds</i> }] [start-time { <i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i> }] Example: <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.

Command or Action	Purpose
Step 4 <code>exit</code> Example: <pre>Router(config)# exit</pre>	Returns to the privileged EXEC mode.
Step 5 <code>show ip sla group schedule</code> Example: <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 6 <code>show ip sla configuration</code> Example: <pre>Router# show ip sla configuration</pre>	(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 <code>enable</code> Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
Step 3 ip sla group schedule <i>group-operation-number operation-id-numbers</i> schedule-period <i>seconds</i> [ageout <i>seconds</i>] [frequency [<i>seconds</i>] range <i>random-frequency-range</i>] [life { forever <i>seconds</i> }] [start-time { <i>hh:mm:ss</i> <i>month day</i> <i>day month</i> } pending now after <i>hh:mm:ss</i> }] Example: Router(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. <ul style="list-style-type: none"> To enable the IP SLAs random scheduler option, you must configure the frequency range <i>random-frequency-range</i> keywords and argument.
Step 4 exit Example: Router(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: Router# show ip sla statistics	(Optional) Displays the IP SLAs operation details.
Step 2	show ip sla group schedule Example: Router# show ip sla group schedule	(Optional) Displays the IP SLAs group schedule details.

	Command or Action	Purpose
Step 3	show ip sla configuration	(Optional) Displays the IP SLAs configuration details.
	Example: Router# show ip sla configuration	

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).

```
Router# 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.

```
Router# 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).

```
Router# 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:

```

Router# 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, page 223](#)
- [Example Enabling the IP SLAs Random Scheduler, page 224](#)

Example Scheduling Multiple IP SLAs Operations

The following example schedules 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.

```
Router# 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).

```

Router# 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	<i>Cisco IOS IP SLAs Command Reference</i>

Standards

Standards	Title
No new or modified standards are supported 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.	--

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 Cisco IOS 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 16 Feature Information for IP SLAs Multiple Operation Scheduling

Feature Name	Releases	Feature Information
IP SLAs Multioperation Scheduler	12.2(31)SB2	The IP SLAs Multioperation Scheduler feature provides a highly scalable infrastructure for Cisco IOS IP SLAs by allowing you to schedule multiple IP SLAs operations using a single command.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
IP SLAs Random Scheduler	12.2(33)SB	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.
	12.2(33)SXI	
	12.3(14)T	
	Cisco IOS XE 3.1.0SG	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



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, page 227](#)
- [Information About Proactive Threshold Monitoring, page 227](#)
- [How to Configure Proactive Threshold Monitoring, page 233](#)
- [Configuration Examples for Proactive Threshold Monitoring, page 236](#)
- [Additional References, page 238](#)
- [Feature Information for IP SLAs Proactive Threshold Monitoring, page 239](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 227](#)
- [IP SLAs Threshold Monitoring and Notifications, page 231](#)

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.

- [Supported Reactions by IP SLAs Operation, page 228](#)

Supported Reactions by IP SLAs Operation

The tables below list which reactions are supported for each IP SLA operation.

Table 17 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	--	--
MaxOfPositiveSD	--	--	Y	--	--	--		Y	--	--
MaxOfNegativeSD	--	--	Y	--	--	--	--	Y	--	--
MaxOfPositiveDS	--	--	Y	--	--	--	--	Y	--	--
MaxOfNegativeDS	--	--	Y	--	--	--	--	Y	--	--
MOS	--	--	Y	--	--	--		--	--	--
ICPIF	--	--	Y	--	--	--	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--	--	--	--

Reaction	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
PacketLossSD	--	--	Y	--	--	--	--	--	--	--
PacketMismatch	--	--	Y	--	--	--	--	--	--	--
iaJitterDS	--	--	--	--	--	--	--	--	--	--
frameLossDS	--	--	--	--	--	--	--	--	--	--
mosLQDSS	--	--	--	--	--	--	--	--	--	--
mosCQDS	--	--	--	--	--	--	--	--	--	--
rfactorDS	--	--	--	--	--	--	--	--	--	--
iaJitterSD	--	--	--	--	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	Y	--	--
LatencyDS	--	--	--	--	--	--	--	Y	--	--
LatencySD	--	--	--	--	--	--	--	Y	--	--
packetLoss	--	--	--	--	--	--	--	Y	--	--

Table 18 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

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
RTTAvg	--	--	--	--	--	--	--	--	--
timeout	Y	Y	Y	Y	--	Y	Y	Y	Y
connection Loss	Y		Y	Y	Y	--	--	Y	--
verifyError	--	--	--	--	--	--	--	--	--
jitterSDAvg	--	--	--	--	--	--	Y	--	--
jitterAvg	--	--	--	--	--	--	Y	--	--
packetLate Arrival	--	--	--	--	--	--	Y	--	--
packetOut OfSequenc e	--	--	--	--	--	--	Y	--	--
MaxOfPos itiveSD	--	--	--	--	--	--	Y	--	--
MaxOfNe gativeSD	--	--	--	--	--	--	Y	--	--
MaxOfPos itiveDS	--	--	--	--	--	--	Y	--	--
MaxOfNe gativeDS	--	--	--	--	--	--	Y	--	--
MOS	--	--	--	--	--	--	--	--	--
ICPIF	--	--	--	--	--	--	--	--	--
PacketLos sDS	--	--	Y	--	--	--	--	--	--
PacketLos sSD	--	--	Y	--	--	--	--	--	--
PacketMI A	--	--	Y	--	--	--	--	--	--
iaJitterDS	--	--	Y	--	--	--	--	--	--
frameLoss DS	--	--	Y	--	--	--	--	--	--

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
mosLQDS	--	--	Y	--	--	--	--	--	--
mosCQDS	--	--	Y	--	--	--	--	--	--
rfactorDS	--	--	Y						
iaJitterSD	--	--	Y	--	--	--	--	--	--
successive PacketLoss	--	--	--	--	--	--	--	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	--	--
LatencyDS	--	--	--	--	--	--	--	--	--
LatencySD	--	--	--	--	--	--	--	--	--
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.

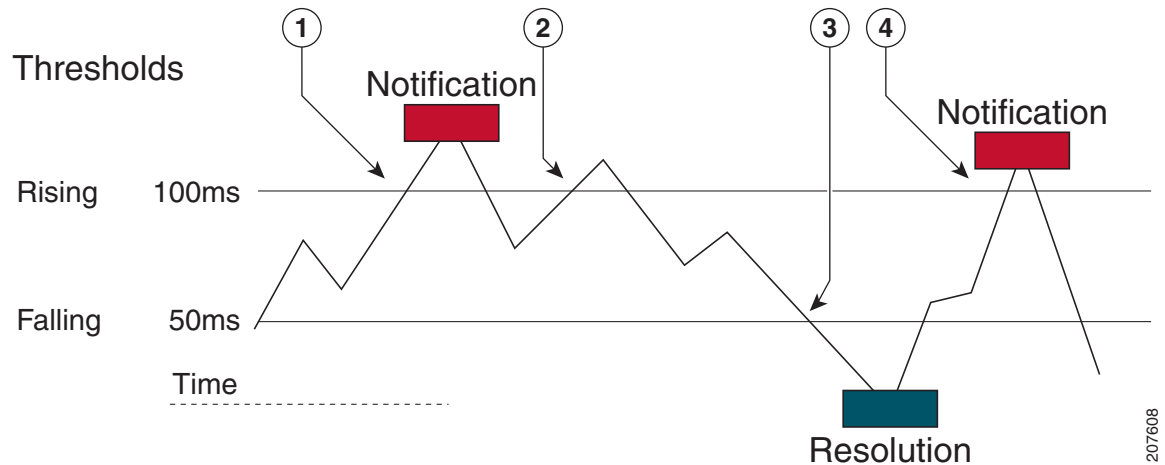
Severity levels in the CISCO-SYSLOG-MIB are defined as follows: SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)}

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 again.

Figure 23



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, page 232](#)

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, page 233](#)

Configuring Proactive Threshold Monitoring

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

- 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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla reaction-configuration <i>operation-number</i> react <i>monitored-element</i> [action-type <i>option</i>] [threshold-type { average [<i>number-of-measurements</i>] consecutive [<i>occurrences</i>] immediate never xofy [<i>x-value</i> <i>y-value</i>]}] [threshold-value <i>upper-threshold</i> <i>lower-threshold</i>] Example: Router(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 <i>operation-number target-operation</i> Example: Router(config)# ip sla reaction-trigger 10 2	(Optional) Starts another IP SLAs operation when the violation conditions are met. <ul style="list-style-type: none"> 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: Router(config)# ip sla logging traps	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 6	Do one of the following: <ul style="list-style-type: none"> snmp-server enable traps rtr snmp-server enable traps syslog Example: Router(config)# snmp-server enable traps rtr Example: Router(config)# snmp-server enable traps syslog	(Optional) Enables system to generate CISCO-RTTMON-MIB traps. or Enables system to generate CISCO-SYSLOG-MIB traps.
Step 7	snmp-server host { <i>hostname ip-address</i> } [vrf <i>vrf-name</i>] [traps informs] [version { 1 2c 3 [auth noauth priv]}] [<i>community-string</i>] [udp-port <i>port</i>] [<i>notification-type</i>] Example: Router(config)# snmp-server host 10.1.1.1 public syslog	(Optional) Sends traps to a remote host. <ul style="list-style-type: none"> Required if the snmp-server enable traps command is configured.
Step 8	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	show ip sla reaction configuration [<i>operation-number</i>] Example: Router# show ip sla reaction configuration 10	(Optional) Displays the configuration of proactive threshold monitoring.

Command or Action	Purpose
Step 10 <code>show ip sla reaction trigger [operation-number]</code> Example: Router# <code>show ip sla reaction trigger 2</code>	(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, page 236](#)
- [Example Verifying an IP SLAs Reaction Configuration, page 236](#)
- [Example Triggering SNMP Notifications, page 237](#)

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):

```
Router(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:

```
Router# show ip sla reaction-configuration 1
Entry number: 1
Reaction Configuration not configured
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip sla reaction-configuration 1
Router(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:

```
Router# 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.
Router(config)# ip sla 1

Router(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
Router(config-ip-sla-jitter)# exit

Router(config)# ip sla schedule 1 start now life forever

! Configure thresholds and reactions.
Router(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly

Router(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly

Router(config)# ip sla logging traps

! The following command sends traps to the specified remote host.
Router(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.
Router(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	<i>Cisco IOS IP SLAs Command Reference</i>

Standards

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

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> 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

RFCs

RFCs	Title
No specific RFCs are supported by the features in this document.	--

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.	http://www.cisco.com/cisco/web/support/index.html
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.	

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 19 Feature Information for IP SLAs Proactive Threshold Monitoring

Feature Name	Releases	Feature Information
IP SLAs Reaction Threshold	12.2(31)SB2	Cisco IOS IP SLAs proactive threshold monitoring capability allows you to configure an IP SLAs operation to react to certain measured network conditions.
	12.2(33)SRB1	
	12.2(33)SXH	
	12.3(14)T	
	15.0(1)S	
	Cisco IOS XE 3.1.0SG	
	12.2(50)SY	

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party

trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.