



IP SLAs Configuration Guide, Cisco IOS Release 15S

First Published: 2012-11-05

Last Modified: 2013-04-02

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

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.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://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. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

IP SLAs Overview 1

Finding Feature Information	1
Information About IP SLAs	1
IP SLAs Technology Overview	1
Service Level Agreements	2
Benefits of IP SLAs	3
Restriction for IP SLAs	4
Network Performance Measurement Using IP SLAs	4
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

CHAPTER 2

Configuring IP SLAs UDP Jitter Operations 11

Finding Feature Information	11
Prerequisites for IP SLAs UDP Jitter Operations	11
Restrictions for IP SLAs UDP Jitter Operations	12
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 a Destination Device	13
Configuring and Scheduling a UDP Jitter Operation on a Source Device	14
Configuring a Basic UDP Jitter Operation on a Source Device	14

Configuring a UDP Jitter Operation with Additional Characteristics	16
Scheduling IP SLAs Operations	19
Troubleshooting Tips	21
What to Do Next	21
Verifying IP SLAs UDP Jitter Operations	21
Configuration Examples for IP SLAs UDP Jitter Operations	24
Example: Configuring a UDP Jitter Operation	24
Additional References for IP SLAs UDP Jitter Operations	25
Feature Information for IP SLAs UDP Jitter Operations	26

CHAPTER 3**IP SLAs Multicast Support** **27**

Finding Feature Information	27
Prerequisites for IP SLAs Multicast Support	27
Restrictions for IP SLAs Multicast Support	28
Information About IP SLAs Multicast Support	28
Multicast UDP Jitter Operations	28
How to Configure IP SLAs Multicast Support	29
Configuring the IP SLAs Responder on a Destination Device	29
Creating a List of Multicast Responders on the Source Device	30
Configuring Multicast UDP Jitter Operations	31
Scheduling IP SLAs Operations	35
Troubleshooting Tips	37
What to Do Next	37
Configuration Examples for IP SLAs Multicast Support	37
Example: Multicast UDP Jitter Operation	37
Additional References for IP SLAs Multicast Support	38
Feature Information for IPSLA Multicast Support	39

CHAPTER 4**Configuring IP SLAs UDP Jitter Operations for VoIP** **41**

Finding Feature Information	41
Restrictions for IP SLAs UDP Jitter Operations for VoIP	42
Information About IP SLAs UDP Jitter Operations for VoIP	42
The Calculated Planning Impairment Factor (ICPIF)	42
Mean Opinion Scores (MOS)	43

Voice Performance Monitoring Using IP SLAs	44
Codec Simulation Within IP SLAs	44
The IP SLAs ICPIF Value	45
The IP SLAs MOS Value	47
How to Configure IP SLAs UDP Jitter Operations for VoIP	47
Configuring the IP SLAs Responder on a Destination Device	47
Configuring and Scheduling an IP SLAs VoIP UDP Jitter Operation	49
Scheduling IP SLAs Operations	52
Troubleshooting Tips	53
What to Do Next	54
Configuration Examples for IP SLAs UDP Jitter Operations for VoIP	54
Example IP SLAs VoIP UDP Operation Configuration	54
Example IP SLAs VoIP UDP Operation Statistics Output	55
Additional References	56
Feature Information for IP SLAs VoIP UDP Jitter Operations	57
Glossary	58
CHAPTER 5	
Configuring IP SLAs LSP Health Monitor Operations	59
Finding Feature Information	59
Prerequisites for LSP Health Monitor Operations	59
Restrictions for LSP Health Monitor Operations	60
Information About LSP Health Monitor Operations	60
Benefits of the LSP Health Monitor	60
How the LSP Health Monitor Works	60
Discovery of Neighboring PE Devices	62
LSP Discovery	63
LSP Discovery Groups	64
IP SLAs LSP Ping and LSP Traceroute	66
Proactive Threshold Monitoring for the LSP Health Monitor	66
Multioperation Scheduling for an LSP Health Monitor	67
How to Configure LSP Health Monitor Operations	68
Configuring an LSP Health Monitor Operation	68
Configuring an LSP Health Monitor Operation without LSP Discovery on a PE Device	68
Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Device	72

Scheduling LSP Health Monitor Operations	76
Troubleshooting Tips	77
What to Do Next	77
Manually Configuring and Scheduling an IP SLAs LSP Ping or LSP Traceroute Operation	77
Troubleshooting Tips	80
What to Do Next	80
Verifying and Troubleshooting LSP Health Monitor Operations	81
Configuration Examples for LSP Health Monitors	83
Example Configuring and Verifying the LSP Health Monitor Without LSP Discovery	83
Example Configuring and Verifying the LSP Health Monitor with LSP Discovery	86
Example Manually Configuring an IP SLAs LSP Ping Operation	89
Additional References	89
Feature Information for LSP Health Monitor Operations	91

CHAPTER 6

IP SLAs for MPLS Psuedo Wire via VCCV	93
Finding Feature Information	93
Restrictions for IP SLAs for MPLS Pseudo Wire via VCCV	93
Information About IP SLAs for MPLS Pseudo Wire via VCCV	93
IP SLAs VCCV Operation	93
Proactive Threshold Monitoring for the LSP Health Monitor	94
How to Configure IP SLAs for MPLS Pseudo Wire via VCCM	95
Manually Configuring and Scheduling an IP SLAs VCCV Operation	95
Troubleshooting Tips	98
What to Do Next	98
Configuration Examples for IP SLAs for MPLS Pseudo Wire via VCCM	98
Example Manually Configuring an IP SLAs VCCV Operation	98
Additional References	99
Feature Information for IP SLAs for MPLS PWE3 via VCCM	101

CHAPTER 7

Configuring IP SLAs for Metro-Ethernet	103
Finding Feature Information	103
Prerequisites for IP SLAs for Metro-Ethernet	103
Restrictions for IP SLAs for Metro-Ethernet	103
Information About IP SLAs for Metro-Ethernet	104

IP SLAs Ethernet Operation Basics	104
How to Configure IP SLAs for Metro-Ethernet	105
Configuring an IP SLAs Auto Ethernet Operation with Endpoint Discovery on the Source Device	
105	
Manually Configuring an IP SLAs Ethernet Ping or Jitter Operation on the Source Device	107
Scheduling IP SLAs Operations	110
Troubleshooting Tips	112
What to Do Next	112
Configuration Examples for IP SLAs for Metro-Ethernet	112
Example IP SLAs Auto Ethernet Operation with Endpoint Discovery	112
Example Individual IP SLAs Ethernet Ping Operation	113
Additional References	113
Feature Information for IP SLAs for Metro-Ethernet	114

CHAPTER 8

Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations	117
Finding Feature Information	117
Prerequisites for ITU-T Y.1731 Operations	117
Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)	118
How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations	118
Configuring a Dual-Ended Ethernet Delay or Delay Variation Operation	118
Configuring a Receiver MEP on the Destination Device	119
Configuring the Sender MEP on the Source Router	121
Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation	123
Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation	126
Scheduling IP SLAs Operations	129
Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations	131
Example: Dual-Ended Ethernet Delay Operation	131
Example: Frame Delay and Frame Delay Variation Measurement Configuration	132
Example: Sender MEP for a Single-Ended Ethernet Delay Operation	133
Example: Sender MEP for a Single-Ended Ethernet Frame Loss Operation	133
Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations	134
Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations	135

CHAPTER 9

IPSLA Y1731 On-Demand and Concurrent Operations	139
--	------------

Finding Feature Information	139
Prerequisites for ITU-T Y.1731 Operations	139
Restrictions for IP SLAs Y.1731 On-Demand Operations	140
Information About IP SLAs Y.1731 On-Demand and Concurrent Operations	140
IPSLA Y1731 SLM Feature Enhancements	140
How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations	141
Configuring a Direct On-Demand Operation on a Sender MEP	141
Configuring a Referenced On-Demand Operation on a Sender MEP	142
Configuring an IP SLAs Y.1731 Concurrent Operation on a Sender MEP	142
Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations	143
Example: On-Demand Operation in Direct Mode	143
Example: On-Demand Operation in Referenced Mode	144
IP SLA Reconfiguration Scenarios	145
Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations	146
Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations	147

CHAPTER 10**Configuring IP SLA - Service Performance Testing** **149**

Finding Feature Information	149
Prerequisites for IP SLA - Service Performance Testing	149
Restrictions for IP SLA - Service Performance Operation	149
Information About IP SLA - Service Performance Testing	150
ITU Y.1564	150
Service Performance Operations	150
How to Configure IP SLA - Service Performance Testing	151
Configuring a Service Performance Operation	151
Configuring Service Performance Profiles on the Sender	153
Scheduling IP SLAs Operations	155
Configuration Examples for IP SLA - Service Performance Testing	157
Example: Service Performance Operation	157
Example: Passive Measurement Mode	158
Additional References for IP SLA - Service Performance Testing	159
Feature Information for IP SLA - Service performance Testing	159

CHAPTER 11**Configuring IP SLAs UDP Echo Operations** **161**

Finding Feature Information	161
Restrictions for IP SLAs UDP Echo Operations	161
Information About IP SLAs UDP Echo Operations	162
UDP Echo Operation	162
How to Configure IP SLAs UDP Echo Operations	163
Configuring the IP SLAs Responder on a Destination Device	163
Configuring a UDP Echo Operation on the Source Device	164
Configuring a Basic UDP Echo Operation on the Source Device	164
Configuring a UDP Echo Operation with Optional Parameters on the Source Device	165
Scheduling IP SLAs Operations	169
Troubleshooting Tips	170
What to Do Next	171
Configuration Examples for IP SLAs UDP Echo Operations	171
Example Configuring a UDP Echo Operation	171
Additional References	171
Feature Information for the IP SLAs UDP Echo Operation	172

CHAPTER 12

Configuring IP SLAs HTTP Operations	173
Finding Feature Information	173
Restrictions for IP SLAs HTTP Operations	173
Information About IP SLAs HTTP Operations	174
HTTP Operation	174
How to Configure IP SLAs HTTP Operations	174
Configuring an HTTP GET Operation on the Source Device	174
Configuring a Basic HTTP GET Operation on the Source Device	175
Configuring an HTTP GET Operation with Optional Parameters on the Source Device	176
Configuring an HTTP RAW Operation on the Source Device	178
Scheduling IP SLAs Operations	179
Troubleshooting Tips	181
What to Do Next	181
Configuration Examples for IP SLAs HTTP Operations	181
Example Configuring an HTTP GET Operation	181
Example Configuring an HTTP RAW Operation	182
Example Configuring an HTTP RAW Operation Through a Proxy Server	182

Example Configuring an HTTP RAW Operation with Authentication	182
Additional References	182
Feature Information for IP SLAs HTTP Operations	183

CHAPTER 13

Configuring IP SLAs TCP Connect Operations	185
Finding Feature Information	185
Information About the IP SLAs TCP Connect Operation	185
TCP Connect Operation	185
How to Configure the IP SLAs TCP Connect Operation	186
Configuring the IP SLAs Responder on the Destination Device	186
Configuring and Scheduling a TCP Connect Operation on the Source Device	187
Prerequisites	187
Configuring a Basic TCP Connect Operation on the Source Device	188
Configuring a TCP Connect Operation with Optional Parameters on the Source Device	189
Configuration Examples for IP SLAs TCP Connect Operations	192
Example Configuring a TCP Connect Operation	192
Additional References	193
Feature Information for the IP SLAs TCP Connect Operation	194

CHAPTER 14

Configuring IP SLAs ICMP Echo Operations	195
Finding Feature Information	195
Restrictions for IP SLAs ICMP Echo Operations	195
Information About IP SLAs ICMP Echo Operations	196
ICMP Echo Operation	196
How to Configure IP SLAs ICMP Echo Operations	196
Configuring an ICMP Echo Operation	196
Configuring a Basic ICMP Echo Operation on the Source Device	196
Configuring an ICMP Echo Operation with Optional Parameters	197
Scheduling IP SLAs Operations	201
Troubleshooting Tips	203
What to Do Next	203
Configuration Examples for IP SLAs ICMP Echo Operations	203
Example Configuring an ICMP Echo Operation	203
Additional References for IP SLAs ICMP Echo Operations	204

CHAPTER 15

Configuring IP SLAs ICMP Path Echo Operations	207
Finding Feature Information	207
Restrictions for IP SLAs ICMP Path Echo Operations	207
Information About IP SLAs ICMP Path Echo Operations	208
ICMP Path Echo Operation	208
How to Configure IP SLAs ICMP Path Echo Operations	208
Configuring an ICMP Path Echo Operation on the Source Device	208
Configuring a Basic ICMP Path Echo Operation on the Source Device	209
Configuring an ICMP Path Echo Operation with Optional Parameters on the Source Device	210
Scheduling IP SLAs Operations	213
Troubleshooting Tips	215
What to Do Next	215
Configuration Examples for IP SLAs ICMP Path Echo Operations	215
Example Configuring an ICMP Path Echo Operation	215
Additional References for IP SLAs ICMP Echo Operations	216
Feature Information for IP SLAs ICMP Path Echo Operations	217

CHAPTER 16

Configuring IP SLAs ICMP Path Jitter Operations	219
Finding Feature Information	219
Prerequisites for ICMP Path Jitter Operations	219
Restrictions for ICMP Path Jitter Operations	220
Information About IP SLAs ICMP Path Jitter Operations	220
ICMP Path Jitter Operation	220
How to Configure the IP SLAs ICMP Path Jitter Operation	221
Configuring the IP SLAs Responder on a Destination Device	221
Configuring an ICMP Path Jitter Operation on the Source Device	222
Configuring a Basic ICMP Path Jitter Operation	222
Configuring an ICMP Path Jitter Operation with Additional Parameters	223
Scheduling IP SLAs Operations	225
Troubleshooting Tips	227
What to Do Next	227
Configuration Examples for IP SLAs ICMP Path Jitter Operations	227

Example Configuring a Path Jitter Operation	227
Additional References	228
Feature Information for IP SLAs ICMP Path Jitter Operations	229
CHAPTER 17	
Configuring IP SLAs FTP Operations	231
Finding Feature Information	231
Restrictions for IP SLAs FTP Operations	231
Information About IP SLAs FTP Operations	232
FTP Operation	232
How to Configure IP SLAs FTP Operations	233
Configuring an FTP Operation on a Source Device	233
Configuring a Basic FTP Operation on the Source Device	233
Configuring an FTP Operation with Optional Parameters on the Source Device	234
Scheduling IP SLAs Operations	236
Troubleshooting Tips	238
What to Do Next	238
Configuration Examples for IP SLAs FTP Operations	238
Example: Configuring an FTP Operation	238
Additional References	239
Feature Information for Configuring IP SLAs FTP Operations	240
CHAPTER 18	
Configuring IP SLAs DNS Operations	241
Finding Feature Information	241
Information About IP SLAs DNS Operations	241
DNS Operation	241
How to Configure IP SLAs DNS Operations	242
Configuring an IP SLAs DNS Operation on the Source Device	242
Configuring a Basic DNS Operation on the Source Device	242
Configuring a DNS Operation with Optional Parameters on the Source Device	243
Scheduling IP SLAs Operations	246
Troubleshooting Tips	248
What to Do Next	248
Configuration Examples for IP SLAs DNS Operations	248
Example Configuring a DNS Operation	248

Additional References	248
Feature Information for Configuring IP SLAs DNS Operation	249

CHAPTER 19**Configuring IP SLAs DHCP Operations** **251**

Finding Feature Information	251
Information About IP SLAs DHCP Operations	251
DHCP Operation	251
IP SLAs DHCP Relay Agent Options	252
How to Configure IP SLAs DHCP Operations	252
Configuring a DHCP Operation on the Source Device	252
Configuring a Basic DHCP Operation	252
Configuring a DHCP Operation with Optional Parameters	253
Scheduling IP SLAs Operations	256
Troubleshooting Tips	257
What to Do Next	257
Configuration Examples for IP SLAs DHCP Operations	258
Example Configuration for an IP SLAs DHCP Operation	258
Additional References	258
Feature Information for IP SLAs DHCP Operations	259

CHAPTER 20**Configuring IP SLAs DLSw+ Operations** **261**

Finding Feature Information	261
Prerequisites	261
Information About IP SLAs DLSw+ Operations	261
DLSw+ Operation	261
How to Configure IP SLAs DLSw+ Operations	262
Configuring IP SLAs DLSw+ Operations	262
Configuring a Basic DLSw+ Operation on the Source Device	262
Configuring an IP SLAs DLSw+ Operation with Optional Parameters on the Source Device	263
Scheduling IP SLAs Operations	266
Troubleshooting Tips	267
What to Do Next	268
Configuration Examples for IP SLAs DLSw+ Operations	268
Example IP SLAs DLSw+ Operation Configuration	268

Additional References	269
Feature Information for Cisco IOS IP SLAs DLSw+ Operations	270

CHAPTER 21

Configuring an IP SLAs Multioperation Scheduler	271
Finding Feature Information	271
Restrictions for an IP SLAs Multioperation Scheduler	271
Prerequisites for an IP SLAs Multioperation Scheduler	271
Information About an IP SLAs Multioperation Scheduler	272
IP SLAs Multioperations Scheduler	272
Default Behavior of IP SLAs Multiple Operations Scheduling	273
IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency	274
Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period	275
IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency	276
IP SLAs Random Scheduler	278
How to Configure an IP SLAs Multioperation Scheduler	279
Scheduling Multiple IP SLAs Operations	279
Enabling the IP SLAs Random Scheduler	280
Verifying IP SLAs Multiple Operations Scheduling	281
Configuration Examples for an IP SLAs Multioperation Scheduler	283
Example Scheduling Multiple IP SLAs Operations	283
Example Enabling the IP SLAs Random Scheduler	283
Additional References	284
Feature Information for a IP SLAs Multioperation Scheduler	284

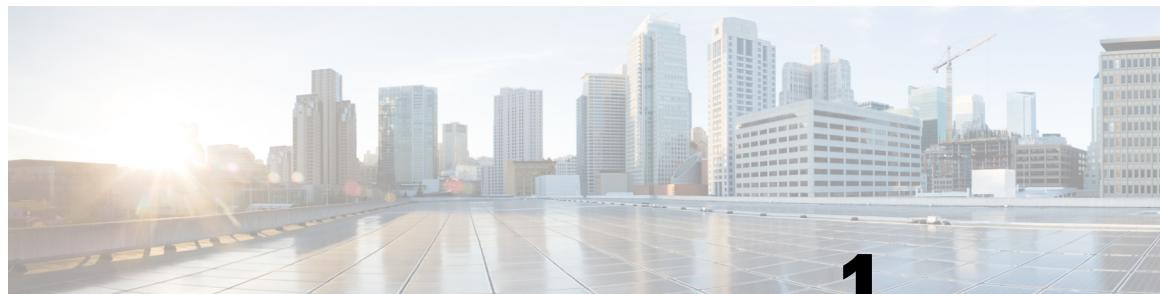
CHAPTER 22

Configuring Proactive Threshold Monitoring for IP SLAs Operations	287
Finding Feature Information	287
Information About Proactive Threshold Monitoring	287
IP SLAs Reaction Configuration	287
Supported Reactions by IP SLAs Operation	288
IP SLAs Threshold Monitoring and Notifications	290
RTT Reactions for Jitter Operations	291
How to Configure Proactive Threshold Monitoring	292
Configuring Proactive Threshold Monitoring	292

Configuration Examples for Proactive Threshold Monitoring	294
Example Configuring an IP SLAs Reaction Configuration	294
Example Verifying an IP SLAs Reaction Configuration	295
Example Triggering SNMP Notifications	295
Additional References	296
Feature Information for IP SLAs Proactive Threshold Monitoring	297

CHAPTER 23**IP SLAs TWAMP Responder** **299**

Finding Feature Information	299
Prerequisites for IP SLAs TWAMP Responder	299
Restrictions for IP SLAs TWAMP Responder	299
Information About IP SLAs TWAMP Responder	300
TWAMP	300
IP SLAs TWAMP Responder v1.0	301
How to Configure an IP SLAs TWAMP Responder	301
Configuring the TWAMP Server	301
Configuring the Session-Reflector	303
Configuration Examples for IP SLAs TWAMP Responder	304
IP SLAs TWAMP Responder v1.0 Example	304
Additional References	304
Feature Information for IP SLAs TWAMP Responder	305



CHAPTER 1

IP SLAs Overview

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

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP SLAs

IP SLAs Technology Overview

Cisco IP SLAs uses active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. IP SLAs sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services, and collects network performance information in real time. The information collected includes data about response time, one-way latency, jitter (interpacket delay variance), packet loss, voice quality scoring, network

Service Level Agreements

resource availability, application performance, and server response time. IP SLAs performs active monitoring by generating and analyzing traffic to measure performance either between Cisco devices or from a Cisco device to a remote IP device such as a network application server. Measurement statistics provided by the various IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

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

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

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

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

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

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

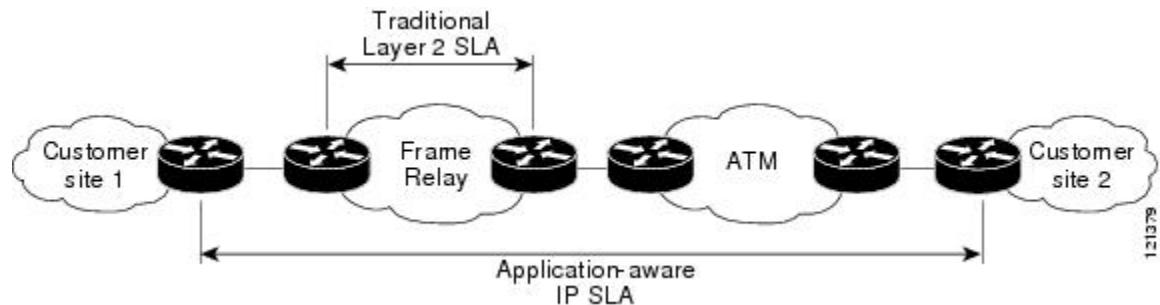
Service Level Agreements

Internet commerce has grown significantly in the past few years as the technology has advanced to provide faster, more reliable access to the Internet. Many companies now need online access and conduct most of their business online and any loss of service can affect the profitability of the company. Internet service

providers (ISPs) and even internal IT departments now offer a defined level of service--a service level agreement--to provide their customers with a degree of predictability.

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

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



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

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

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

Benefits of IP SLAs

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

■ Restriction for IP SLAs

- 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

Restriction for IP SLAs

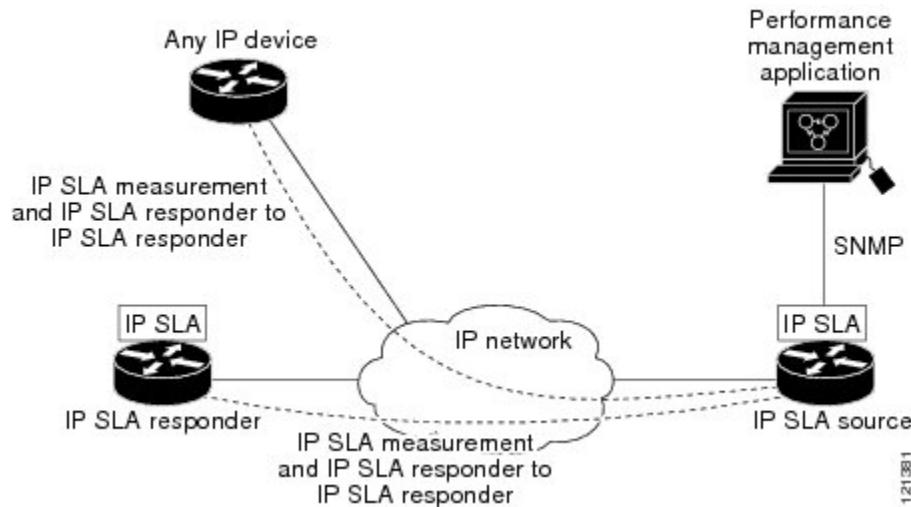
IP SLAs configured with *start-time now* keyword need to be restarted after reload.

Network Performance Measurement Using IP SLAs

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

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

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

Figure 2: IP SLAs Operations

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

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

IP SLAs Responder and IP SLAs Control Protocol

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

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

Enabling the IP SLAs Responder on the destination device is not required for all IP SLAs operations. For example, if services that are already provided by the destination device (such as Telnet or HTTP) are chosen,

Response Time Computation for IP SLAs

the IP SLAs Responder need not be enabled. For non-Cisco devices, the IP SLAs Responder cannot be configured and IP SLAs can send operational packets only to services native to those devices.

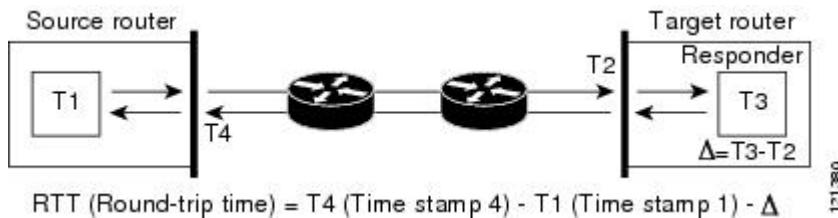
Response Time Computation for IP SLAs

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

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

The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.

Figure 3: IP SLAs Responder Time Stamping



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

IP SLAs Operation Scheduling

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

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

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

IP SLAs Operation Threshold Monitoring

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

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency

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

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

MPLS VPN Awareness

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

History Statistics

IP SLAs maintains the following three types of history statistics:

- Aggregated statistics--By default, IP SLAs maintains two hours of aggregated statistics for each operation. Value from each operation cycle is aggregated with the previously available data within a given hour. The Enhanced History feature in IP SLAs allows for the aggregation interval to be shorter than an hour.

Additional References

- 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
IP SLAs commands	<i>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

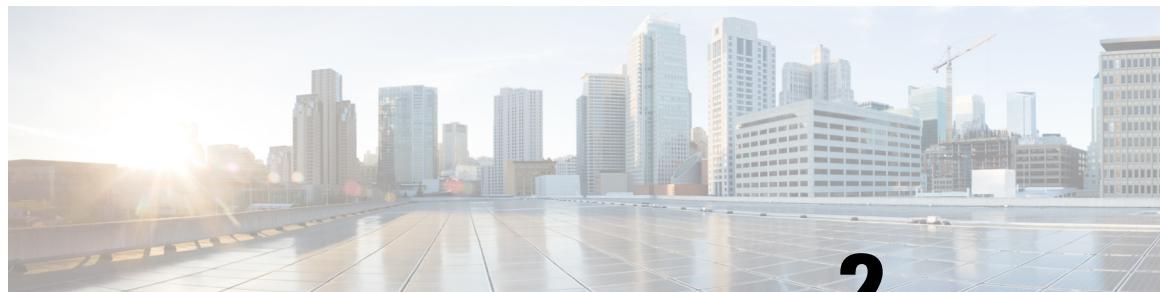
RFCs

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

Additional References



CHAPTER 2

Configuring IP SLAs UDP Jitter Operations

This document describes how to configure an IP Service Level Agreements (SLAs) UDP jitter operation to analyze round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic in IPv4 or IPv6 networks. This module also explains how the data gathered using the UDP jitter operation can be displayed and analyzed using Cisco software commands.

- [Finding Feature Information, on page 11](#)
- [Prerequisites for IP SLAs UDP Jitter Operations, on page 11](#)
- [Restrictions for IP SLAs UDP Jitter Operations, on page 12](#)
- [Information About IP SLAs UDP Jitter Operations, on page 12](#)
- [How to Configure IP SLAs UDP Jitter Operations, on page 13](#)
- [Verifying IP SLAs UDP Jitter Operations, on page 21](#)
- [Configuration Examples for IP SLAs UDP Jitter Operations, on page 24](#)
- [Additional References for IP SLAs UDP Jitter Operations, on page 25](#)
- [Feature Information for IP SLAs UDP Jitter Operations, on page 26](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP SLAs UDP Jitter Operations

- Time synchronization, such as that provided by the Network Time Protocol (NTP), is required between the source and the target device to provide accurate one-way delay (latency) measurements. To configure NTP on source and target devices, perform the tasks in the “Performing Basic System Management” chapter of the *Basic System Management Configuration Guide*. Time synchronization is not required for one-way jitter and packet loss measurements. If time is not synchronized between source and target devices, one-way jitter and packet loss data are returned, but values of “0” are returned for the one-way delay measurements provided by the UDP jitter operation.

■ Restrictions for IP SLAs UDP Jitter Operations

- Before configuring any IP Service Level Agreements (SLAs) application, use the **show ip sla application** command to verify that the operation type is supported on the software image.

Restrictions for IP SLAs UDP Jitter Operations

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

Information About IP SLAs UDP Jitter Operations

IP SLAs UDP Jitter Operation

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

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

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

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

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

The UDP jitter operation functions by generating synthetic (simulated) UDP traffic. Asymmetric probes support custom-defined packet sizes per direction with which different packet sizes can be sent in request packets (from the source device to the destination device) and in response packets (from the destination device to the source device).

The UDP jitter operation sends N number of UDP packets, each of size S, T milliseconds apart, from a source device to a destination device, at a given frequency of F. In response, UDP packets of size P is sent from the destination device to the source device. By default, ten packet frames (N), each with a payload size of 10 bytes (S), are generated every 10 ms (T), and the operation is repeated every 60 seconds (F). Each of these

parameters is user-configurable, so as to best simulate the IP service that you provide, as shown in the table below.

Table 1: UDP Jitter Operation Parameters

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

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

How to Configure IP SLAs UDP Jitter Operations

Configuring the IP SLAs Responder on a Destination Device



Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress ip-address port portvrf vrf**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: • ip sla responder • ip sla responder udp-echo ipaddress ip-address port portvrf vrf Example: Device(config)# ip sla responder Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1	(Optional) Temporarily enables IP SLAs responder functionality on a Cisco device in response to control messages from the source. (Optional; required only if protocol control is disabled on the source.) Enables IP SLAs responder functionality on the specified IP address, port and VRF. • Protocol control is enabled by default.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a UDP Jitter Operation on a Source Device

Perform only one of the following tasks:

- [Configuring a Basic UDP Jitter Operation on a Source Device](#)
- [Configuring a UDP Jitter Operation with Additional Characteristics](#)

Configuring a Basic UDP Jitter Operation on a Source Device**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **udp-jitter {destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval interpacket-interval]**
5. **frequency seconds**

6. **end**
7. **show ip sla configuration [operation-number]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Starts configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	udp-jitter {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname}] [source-port port-number] [control {enable disable}] [num-packets number-of-packets] [interval interpacket-interval] Example: Device(config-ip-sla)# udp-jitter 192.0.2.135 5000	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter 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 source and destination devices.
Step 5	frequency seconds Example: Device(config-ip-sla-jitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-jitter)# end	Exits UDP Jitter configuration mode and returns to privileged EXEC mode.
Step 7	show ip sla configuration [operation-number] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

What to do next

To configure the percentile option for your operation, see the “Configuring the IP SLAs—Percentile Support for Filtering Outliers” module.

Configuring a UDP Jitter Operation with Additional Characteristics

**Note**

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

Before you begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **udp-jitter {destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval interpacket-interval]**
5. **history distributions-of-statistics-kept size**
6. **history enhanced [interval seconds] [buckets number-of-buckets]**
7. **frequency seconds**
8. **history hours-of-statistics-kept hours**
9. **owner owner-id**
10. **request-data-size bytes**
11. **response-data-size bytes**
12. **history statistics-distribution-interval milliseconds**
13. **tag text**
14. **threshold milliseconds**
15. **timeout milliseconds**
16. Enter one of the following commands:
 - **tos number**
 - **traffic-class number**

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	udp-jitter {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname}] [source-port port-number] [control {enable disable}] [num-packets number-of-packets] [interval interpacket-interval] Example: Device(config-ip-sla)# udp-jitter 192.0.2.134 5000	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration mode. • Use the control disable keyword combination only if you disable the IP SLAs control protocol on both source and target devices.
Step 5	history distributions-of-statistics-kept size Example: Device(config-ip-sla-jitter)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop for an IP SLAs operation.
Step 6	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-jitter)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 7	frequency seconds Example:	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

Configuring a UDP Jitter Operation with Additional Characteristics

	Command or Action	Purpose
	Device(config-ip-sla-jitter)# frequency 30	
Step 8	history hours-of-statistics-kept hours Example: Device(config-ip-sla-jitter)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 9	owner owner-id Example: Device(config-ip-sla-jitter)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 10	request-data-size bytes Example: Device(config-ip-sla-jitter)# request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation request packet.
Step 11	response-data-size bytes Example: Device(config-ip-sla-jitter)# response-data-size 25	(Optional) Sets the protocol data size in the payload of an IP SLAs operation response packet.
Step 12	history statistics-distribution-interval milliseconds Example: Device(config-ip-sla-jitter)# history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 13	tag text Example: Device(config-ip-sla-jitter)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 14	threshold milliseconds Example: Device(config-ip-sla-jitter)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 15	timeout milliseconds Example: Device(config-ip-sla-jitter)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.

	Command or Action	Purpose
Step 16	Enter one of the following commands: <ul style="list-style-type: none"> • tos number • traffic-class number Example: Device(config-ip-sla-jitter)# tos 160 Device(config-ip-sla-jitter)# traffic-class 160	(Optional) Defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) Defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.
Step 17	flow-label number Example: Device(config-ip-sla-jitter)# flow-label 112233	(Optional) Defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 18	verify-data Example: Device(config-ip-sla-jitter)# verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 19	vrf vrf-name Example: Device(config-ip-sla-jitter)# vrf vpn-A	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) VPNs using IP SLAs operations.
Step 20	end Example: Device(config-ip-sla-jitter)# end	Exits UDP jitter configuration mode and returns to privileged EXEC mode.
Step 21	show ip sla configuration [operation-number] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

What to do next

To configure the percentile option for your operation, see the “Configuring the IP SLAs—Percentile Support for Filtering Outliers” module.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.

- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

- enable**
- configure terminal**
- Enter one of the following commands:
 - ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
- end**
- show ip sla group schedule**
- show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now</pre>	<ul style="list-style-type: none"> Configures the scheduling parameters for an individual IP SLAs operation. Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

	Command or Action	Purpose
	<pre>Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: <pre>Device# show ip sla configuration</pre>	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Verifying IP SLAs UDP Jitter Operations

SUMMARY STEPS

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

3. **show ip sla group schedule**
4. **show ip sla statistics**
5. **show ip sla statistics 2 details**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show ip sla configuration**

Displays IP SLAs configuration details.

Example:

```
Device# show ip sla configuration

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

Step 3 **show ip sla group schedule**

Displays IP SLAs group schedule details.

Example:

```
Device# show ip sla group schedule

Group Entry Number: 1
Probes to be scheduled: 6-9,3-4
Total number of probes: 6
Schedule period: 10
Mode: even
Group operation frequency: Equals schedule period
```

```
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Pending trigger
Life (seconds): 3600
Entry Ageout (seconds): never
```

Step 4 show ip sla statistics

Displays IP SLAs statistics.

Example:

```
Device# show ip sla statistics

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

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

Step 5 show ip sla statistics 2 details

Displays IPSLAs latest operation statistics

Example:

```
Device# show ip sla statistics 2 details

IPSLA operation id: 2
Type of operation: udp-jitter
Latest RTT: 1 milliseconds
Latest operation start time: 07:45:28 GMT Thu Aug 28 2014
Latest operation return code: OK
Over thresholds occurred: FALSE
RTT Values:
Number Of RTT: 10 RTT Min/Avg/Max: 1/1/1 milliseconds
Latency one-way time:
Number of Latency one-way Samples: 6
Source to Destination Latency one way Min/Avg/Max: 1/1/1 milliseconds
Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
```

Configuration Examples for IP SLAs UDP Jitter Operations

```

Source to Destination Latency one way Sum/Sum2: 6/6
Destination to Source Latency one way Sum/Sum2: 0/0
Jitter Time:
Number of SD Jitter Samples: 9
Number of DS Jitter Samples: 9
Source to Destination Jitter Min/Avg/Max: 0/1/1 milliseconds
Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Source to destination positive jitter Min/Avg/Max: 1/1/1 milliseconds
Source to destination positive jitter Number/Sum/Sum2: 3/3/3
Source to destination negative jitter Min/Avg/Max: 1/1/1 milliseconds
Source to destination negative jitter Number/Sum/Sum2: 3/3/3
Destination to Source positive jitter Min/Avg/Max: 0/0/0 milliseconds
Destination to Source positive jitter Number/Sum/Sum2: 0/0/0
Destination to Source negative jitter Min/Avg/Max: 0/0/0 milliseconds
Destination to Source negative jitter Number/Sum/Sum2: 0/0/0
Interarrival jitterout: 0 Interarrival jitterin: 0
Jitter AVG: 1
Over Threshold:
Number Of RTT Over Threshold: 0 (0%)
Packet Loss Values:
Loss Source to Destination: 0
Source to Destination Loss Periods Number: 0
Source to Destination Loss Period Length Min/Max: 0/0
Source to Destination Inter Loss Period Length Min/Max: 0/0
Loss Destination to Source: 0
Destination to Source Loss Periods Number: 0
Destination to Source Loss Period Length Min/Max: 0/0
Destination to Source Inter Loss Period Length Min/Max: 0/0
Out Of Sequence: 0 Tail Drop: 0 Packet Late Arrival: 0
Packet Skipped: 0
Voice Score Values:
Calculated Planning Impairment Factor (ICPIF): 0
Mean Opinion Score (MOS): 0
Number of successes: 2
Number of failures: 0
Operation time to live: Forever
Operational state of entry: Active
Last time this entry was reset: Never

```

Configuration Examples for IP SLAs UDP Jitter Operations

Example: Configuring a UDP Jitter Operation

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

```

configure terminal
ip sla 1
  udp-jitter 192.0.2.115 65051 num-packets 20
    request-data-size 160
    tos 128
    frequency 30
  ip sla schedule 1 start-time after 00:05:00
  ip sla 2
    udp-jitter 192.0.2.115 65052 num-packets 20 interval 10
      request-data-size 20

```

```

tos 64
frequency 30
ip sla schedule 2 start-time after 00:05:05

```

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

```
ip sla responder
```

Additional References for IP SLAs UDP Jitter Operations

Related Documents

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

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> • CISCO-DATA-COLLECTION-MIB • CISCO-RTTMON-MIB • IPV6-FLOW-LABEL-MIB 	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs UDP Jitter Operations

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

Feature Name	Releases	Feature Information
IP SLAs—UDP Jitter Operation	Cisco IOS 12.2(31)SB2 Cisco IOS 12.2(33)SRB1 Cisco IOS 12.2(33)SXH Cisco IOS 12.3(14)T Cisco IOS 15.0(1)S	The IP SLAs UDP jitter operation allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.
IP SLAs for IPv6 (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	Cisco IOS 12.2(33)SRC Cisco IOS 12.2(33)SB Cisco IOS 12.4(20)T Cisco IOS 12.2(50)SY	The IP SLAs for IPv6 (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect) feature adds support for operability in IPv6 networks.
IP SLAs—Asymmetric Probe Support for UDP Jitter	Cisco IOS 15.3(3)M Cisco IOS 15.3(3)S	The IP SLAs—Asymmetric Probe Support for UDP Jitter feature supports the configuration of custom-defined packet sizes in response packets. The following command was introduced: response-data-size .



CHAPTER 3

IP SLAs Multicast Support

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

- [Finding Feature Information, on page 27](#)
- [Prerequisites for IP SLAs Multicast Support, on page 27](#)
- [Restrictions for IP SLAs Multicast Support, on page 28](#)
- [Information About IP SLAs Multicast Support, on page 28](#)
- [How to Configure IP SLAs Multicast Support, on page 29](#)
- [Configuration Examples for IP SLAs Multicast Support, on page 37](#)
- [Additional References for IP SLAs Multicast Support, on page 38](#)
- [Feature Information for IPSLA Multicast Support, on page 39](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP SLAs Multicast Support

- Time synchronization, such as that provided by Network Time Protocol (NTP), is required between the source and the target device in order to provide accurate one-way delay (latency) measurements. To configure NTP on the source and target devices, perform the tasks in the "Performing Basic System Management" chapter of the *Network Management Configuration Guide*. Time synchronization is not required for the one-way jitter and packet loss measurements. However, if the time is not synchronized between the source and target devices, one-way jitter and packet loss data will be returned, but values of "0" will be returned for the one-way delay measurements provided by the UDP jitter operation.
- All devices must be part of the same VRF in order for IP SLAs multicast operations to succeed.

■ Restrictions for IP SLAs Multicast Support

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

Restrictions for IP SLAs Multicast Support

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

Information About IP SLAs Multicast Support

Multicast UDP Jitter Operations

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

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

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

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

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

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

Multicast UDP jitter operations are supported in IPv4 networks.

How to Configure IP SLAs Multicast Support

Configuring the IP SLAs Responder on a Destination Device


Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress ip-address port portvrf vrf**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla responder • ip sla responder udp-echo ipaddress ip-address port portvrf vrf Example: Device(config)# ip sla responder Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1	(Optional) Temporarily enables IP SLAs responder functionality on a Cisco device in response to control messages from the source. (Optional; required only if protocol control is disabled on the source.) Enables IP SLAs responder functionality on the specified IP address, port and VRF. • Protocol control is enabled by default.

Creating a List of Multicast Responders on the Source Device

	Command or Action	Purpose
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.

Creating a List of Multicast Responders on the Source Device

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla endpoint-list type ip <i>template-name</i> Example: <pre>Device(config)# ip sla endpoint-list type ip mcast-rcvrs</pre>	Begins configuring an endpoint list and enters endpoint-list configuration mode.
Step 4	description <i>description</i> Example:	(Optional) Adds descriptive text to the template being configured.

	Command or Action	Purpose
	Device(config-epl)# description list of receivers	
Step 5	ip-address address [-address , ... , address] port port Example: Device(config-epl)# ip-address 10.1.1.1-13 port 6500	Adds the IPv4 or IPv6 address of a multicast responder to the endpoint list being configured. <ul style="list-style-type: none"> • Repeat this command until all desired addresses are configured. • Use the no form of this command to modify the endpoint list by removing one or more addresses.
Step 6	end Example: Device(config-epl)# end	Returns to privileged EXEC mode.
Step 7	show ip sla endpoint-list [type ip [template-name]] Example: Device# show ip sla endpoint-list type ip mcast-rcvrs	(Optional) Displays the configuration of the endpoint list.

Configuring Multicast UDP Jitter Operations


Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **udp-jitter {destination-ip-address | destination-hostname} destination-port endpoint-list endpoint-list [ssm] [source-ip ip-address] [source-port port-number] [num-packets number-of-packets] [interval interpacket-interval]**
5. **control retry retries**
6. **control timeout seconds**
7. **dscp dscp-value**

8. **tree-init number**
9. **history distributions-of-statistics-kept size**
10. **history enhanced [interval seconds] [buckets number-of-buckets]**
11. **frequency seconds**
12. **history hours-of-statistics-kept hours**
13. **owner owner-id**
14. **request-data-size bytes**
15. **history statistics-distribution-interval milliseconds**
16. **tag text**
17. **threshold milliseconds**
18. **timeout milliseconds**
19. **tos number**
20. **verify-data**
21. **vrf vrf-name**
22. **end**
23. **show ip sla configuration [operation-number]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config)# ip sla 10</pre>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	udp-jitter {destination-ip-address destination-hostname} destination-port endpoint-list endpoint-list [ssm] [source-ip ip-address] [source-port port-number] [num-packets number-of-packets] [interval interpacket-interval] Example: <pre>Device(config-ip-sla)# udp-jitter 239.1.1.1 5000 endpoint-list mcast-rcvrs source-ip 10.10.10.106 source-port 7012 num-packets 50 interval 25</pre>	Configures the IP SLAs operation as a multicast UDP jitter operation and enters multicast UDP jitter configuration mode.

	Command or Action	Purpose
Step 5	control retry <i>retries</i> Example: Device(config-ip-sla-multicast-jitter-oper)# control retry 2	(Optional) Configures the number of times a sending device will resend a control protocol message.
Step 6	control timeout <i>seconds</i> Example: Device(config-ip-sla-multicast-jitter)# control timeout 4	(Optional) Configures the number of seconds that the destination device will wait for a control protocol message.
Step 7	dscp <i>dscp-value</i> Example: Device(config-ip-sla-multicast-jitter-oper)# dscp 10	(Optional) Configures the DSCP value for the operation.
Step 8	tree-init <i>number</i> Example: Device(config-ip-sla-multicast-jitter-oper)# tree-init 1	(Optional) Sets up the multicast tree.
Step 9	history distributions-of-statistics-kept <i>size</i> Example: Device(config-ip-sla-multicast-jitter-oper)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 10	history enhanced [<i>interval seconds</i>] [<i>buckets number-of-buckets</i>] Example: Device(config-ip-sla-multicast-jitter-oper)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 11	frequency <i>seconds</i> Example: Device(config-ip-sla-multicast-jitter-oper)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 12	history hours-of-statistics-kept <i>hours</i> Example: Device(config-ip-sla-multicast-jitter-oper)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 13	owner <i>owner-id</i> Example:	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.

Configuring Multicast UDP Jitter Operations

	Command or Action	Purpose
	Device(config-ip-sla-multicast-jitter-oper) # owner admin	
Step 14	request-data-size bytes Example: Device(config-ip-sla-multicast-jitter-oper) # request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	history statistics-distribution-interval milliseconds Example: Device(config-ip-sla-multicast-jitter-oper) # history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	tag text Example: Device(config-ip-sla-multicast-jitter-oper) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	threshold milliseconds Example: Device(config-ip-sla-multicast-jitter-oper) # threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	timeout milliseconds Example: Device(config-ip-sla-multicast-jitter-oper) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	tos number Example: Device(config-ip-sla-multicast-jitter-oper) # tos 160	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 20	verify-data Example: Device(config-ip-sla-multicast-jitter-oper) # verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 21	vrf vrf-name Example:	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) VPNs using IP SLAs operations.

	Command or Action	Purpose
	Device(config-ip-sla-multicast-jitter-oper) # vrf vpn-A	
Step 22	end Example: Device(config-ip-sla-multicast-jitter-oper) # end	Returns to privileged EXEC mode.
Step 23	show ip sla configuration [operation-number] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month]} | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {[hh:mm [:ss] [month day | day month]} | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

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

Scheduling IP SLAs Operations

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: <pre>Device# show ip sla configuration</pre>	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs Multicast Support

Example: Multicast UDP Jitter Operation

```
Device# show ip sla endpoint-list

Endpoint-list Name: multicast
  Description:
    ip-address 192.0.2.1 port 1111
    ip-address 192.0.2.2 port 2222
    ip-address 192.0.2.3 port 3333

Device# show ip sla configuration 22

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

Additional References for IP SLAs Multicast Support

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

Enhanced History:

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

Additional References for IP SLAs Multicast Support

Related Documents

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

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPSLA Multicast Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for IPSLA Multicast Support

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



CHAPTER 4

Configuring IP SLAs UDP Jitter Operations for VoIP

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



Note

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

- [Finding Feature Information, on page 41](#)
- [Restrictions for IP SLAs UDP Jitter Operations for VoIP, on page 42](#)
- [Information About IP SLAs UDP Jitter Operations for VoIP, on page 42](#)
- [How to Configure IP SLAs UDP Jitter Operations for VoIP, on page 47](#)
- [Configuration Examples for IP SLAs UDP Jitter Operations for VoIP, on page 54](#)
- [Additional References, on page 56](#)
- [Feature Information for IP SLAs VoIP UDP Jitter Operations, on page 57](#)
- [Glossary, on page 58](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs UDP Jitter Operations for VoIP

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

Information About IP SLAs UDP Jitter Operations for VoIP

The Calculated Planning Impairment Factor (ICPIF)

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

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

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

where

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

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

Table 4: Quality Levels as a Function of Total Impairment Factor ICPIF

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

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


Note

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

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

Mean Opinion Scores (MOS)

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

Table 5: MOS Ratings

Score	Quality	Description of Quality Impairment
5	Excellent	Imperceptible
4	Good	Just perceptible, but not annoying
3	Fair	Perceptible and slightly annoying
2	Poor	Annoying but not objectionable

Score	Quality	Description of Quality Impairment
1	Bad	Very annoying and objectionable

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

Voice Performance Monitoring Using IP SLAs

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

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

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

Codec Simulation Within IP SLAs

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

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

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

Table 6: Default VoIP UDP Jitter Operation Parameters by Codec

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

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

The IP SLAs ICPIF Value

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

$$\text{Total Impairment Factor (Icpif)} = \text{Delay Impairment Factor (Idd)} + \text{Equipment Impairment Factor (Ie)} - \text{Expectation/Advantage Factor (A)}$$

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

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

The Delay Impairment Factor

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

Table 7: Sample Correspondence of One-Way Delay to ICPIF Delay Impairment

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

One-Way Delay (ms)	Delay Impairment Factor
200	7

The Equipment Impairment Factor

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

Table 8: Sample Correspondence of Measured Packet Loss to ICPiF Equipment Impairment

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

The Expectation Factor

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

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

Table 9: Advantage Factor Recommended Maximum Values

Communication Service	Advantage / Expectation Factor: Maximum value of A
Conventional wire-line (land-line)	0
Mobility (cellular connections) within a building	5
Mobility within a Geographical area or moving in a vehicle	10
Access to hard-to-reach location; (for example, via multi-hop satellite connections)	20

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

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

The IP SLAs MOS Value

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

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

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

Table 10: Correspondence of ICPIF Values to MOS Values

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

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

How to Configure IP SLAs UDP Jitter Operations for VoIP

Configuring the IP SLAs Responder on a Destination Device



Note

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

SUMMARY STEPS

- enable

- 2. configure terminal**
- 3.** Enter one of the following commands:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress ip-address port portvrf vrf**
- 4. end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla responder • ip sla responder udp-echo ipaddress ip-address port portvrf vrf Example: <pre>Device(config)# ip sla responder</pre> <pre>Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1</pre>	<ul style="list-style-type: none"> (Optional) Temporarily enables IP SLAs responder functionality on a Cisco device in response to control messages from the source. (Optional; required only if protocol control is disabled on the source.) Enables IP SLAs responder functionality on the specified IP address, port and VRF. • Protocol control is enabled by default.
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling an IP SLAs VoIP UDP Jitter Operation


Note

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

SUMMARY STEPS

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

17. show ip sla configuration [operation-number]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	udp-jitter {destination-ip-address destination-hostname} destination-port codec codec-type [codec-numpackets number-of-packets] [codec-size number-of-bytes] [codec-interval milliseconds] [advantage-factor value] [source-ip {ip-address hostname}] [source-port port-number] [control {enable disable}] Example: Device(config-ip-sla)# udp-jitter 209.165.200.225 16384 codec g711alaw advantage-factor 10	Configures the operation as a jitter (codec) operation that will generate VoIP scores in addition to latency, jitter, and packet loss statistics.
Step 5	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-jitter)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 6	frequency seconds Example: Device(config-ip-sla-jitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 7	history hours-of-statistics-kept hours Example: Device(config-ip-sla-jitter)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.

	Command or Action	Purpose
Step 8	owner owner-id Example: Device(config-ip-sla-jitter)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 9	tag text Example: Device(config-ip-sla-jitter)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 10	threshold milliseconds Example: Device(config-ip-sla-jitter)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 11	timeout milliseconds Example: Device(config-ip-sla-jitter)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 12	Do one of the following: • tos number • traffic-class number Example: Device(config-ip-sla-jitter)# tos 160 Example: Device(config-ip-sla-jitter)# traffic-class 160	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.
Step 13	flow-label number Example: Device(config-ip-sla-jitter)# flow-label 112233	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 14	verify-data Example: Device(config-ip-sla-jitter)# verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 15	vrf vrf-name Example: Device(config-ip-sla-jitter)# vrf vpn-A	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.

	Command or Action	Purpose
Step 16	end Example: Device(config-ip-sla-jitter)# end	Returns to privileged EXEC mode.
Step 17	show ip sla configuration [operation-number] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

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

	Command or Action	Purpose
	Device# configure terminal	
Step 3	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] <p>Example:</p> <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for

What to Do Next

corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.

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

What to Do Next

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

Configuration Examples for IP SLAs UDP Jitter Operations for VoIP

Example IP SLAs VoIP UDP Operation Configuration

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

```
Device> enable
Password:
Device# configure terminal

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

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

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

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

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

Entry number: 10
Owner: admin_bofh
Tag:
Type of operation to perform: jitter
Target address: 209.165.200.225
Source address: 0.0.0.0
Target port: 16384
```

```

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

```

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

Example IP SLAs VoIP UDP Operation Statistics Output

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

```

Device# show ip sla statistics 10

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

```

Additional References

```

RTTSum: 191      RTTSum2: 3649
Packet Loss Values:
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0   PacketMIA: 0      PacketLateArrival: 0
InternalError: 0        Busies: 0
Jitter Values:
NumOfJitterSamples: 9
MinOfPositivesSD: 0    MaxOfPositivesSD: 0
NumOfPositivesSD: 0    SumOfPositivesSD: 0    Sum2PositivesSD: 0
MinOfNegativesSD: 0    MaxOfNegativesSD: 0
NumOfNegativesSD: 0    SumOfNegativesSD: 0    Sum2NegativesSD: 0
MinOfPositivesDS: 1    MaxOfPositivesDS: 1
NumOfPositivesDS: 1    SumOfPositivesDS: 1    Sum2PositivesDS: 1
MinOfNegativesDS: 1    MaxOfNegativesDS: 1
NumOfNegativesDS: 1    SumOfNegativesDS: 1    Sum2NegativesDS: 1
Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
NumOfOW: 0
OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference
Voice over IP (VoIP) codecs	Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation
Jitter in Packet Voice Networks	Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms) shtml

Standards and RFCs

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

Standard ¹ /RFC ²	Title
RFC 768	<i>User Datagram Protocol</i>
RFC 1889	<i>RTP: A Transport Protocol for Real-Time Applications</i>

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

² Full support by this feature for listed RFCs is not claimed.

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs VoIP UDP Jitter Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11: Feature Information for the IP SLAs VoIP UDP Jitter Operation

Feature Name	Releases	Feature Information
IP SLAs - UDP Based VoIP Operation	Cisco IOS 12.2(31)SB2 Cisco IOS 12.2(33)SRB1 Cisco IOS 12.2(33)SXH Cisco IOS 12.3(14)T Cisco IOS XE Release 2.1 Cisco IOS 15.0(1)S	The IP SLAs User Datagram Protocol (UDP) jitter operation allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.
IP SLAs for IPv6 (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	Cisco IOS 12.2(33)SRC Cisco IOS 12.2(33)SB Cisco IOS 12.4(2)T Cisco IOS XE Release 2.1	Support was added for operability in IPv6 networks.

Glossary

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

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

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

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

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

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

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



CHAPTER 5

Configuring IP SLAs LSP Health Monitor Operations

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

- [Finding Feature Information, on page 59](#)
- [Prerequisites for LSP Health Monitor Operations, on page 59](#)
- [Restrictions for LSP Health Monitor Operations, on page 60](#)
- [Information About LSP Health Monitor Operations, on page 60](#)
- [How to Configure LSP Health Monitor Operations, on page 68](#)
- [Configuration Examples for LSP Health Monitors, on page 83](#)
- [Additional References, on page 89](#)
- [Feature Information for LSP Health Monitor Operations, on page 91](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for LSP Health Monitor Operations

- The participating PE devices of an LSP Health Monitor operation must support the MPLS LSP ping feature. It is recommended that the Provider (P) devices also support the MPLS LSP Ping feature in order to obtain complete error reporting and diagnostics information.

Restrictions for LSP Health Monitor Operations

- Ensure that the source PE device has enough memory to support the desired LSP Health Monitor functionality. Enabling the LSP discovery option can potentially have a significant impact on device memory. If there is not enough memory available during the LSP discovery process, the process will gracefully terminate and an error message will be displayed.



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

Restrictions for LSP Health Monitor Operations

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

Information About LSP Health Monitor Operations

Benefits of the LSP Health Monitor

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

How the LSP Health Monitor Works

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

1. The user configures an LSP Health Monitor operation and the BGP next hop neighbor discovery process is enabled.

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

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

**Note**

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

2. The user configures proactive threshold monitoring parameters for the LSP Health Monitor operation. For more information about proactive threshold monitoring, see the "Proactive Threshold Monitoring for the LSP Health Monitor" section.

Depending on the proactive threshold monitoring configuration options chosen, SNMP trap notifications or syslog messages are generated as threshold violations are met.

3. The user configures multioperation scheduling parameters for the LSP Health Monitor operation. For more information about multioperation scheduling, see the "Multioperation Scheduling for the LSP Health Monitor" section.

Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created (based on parameters configured in Step 1) for each applicable PE (BGP next hop) neighbor. The IP SLAs operations will measure network connectivity between the source PE device and the discovered destination PE device. The start time and frequency of each measurement is based on the multioperation scheduling parameters defined by the user.

Addition and Deletion of IP SLAs Operations

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

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

Access Lists for Filtering BGP Next Hop Neighbors

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

Unique Identifier for Each Automatically Created IP SLAs Operation

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

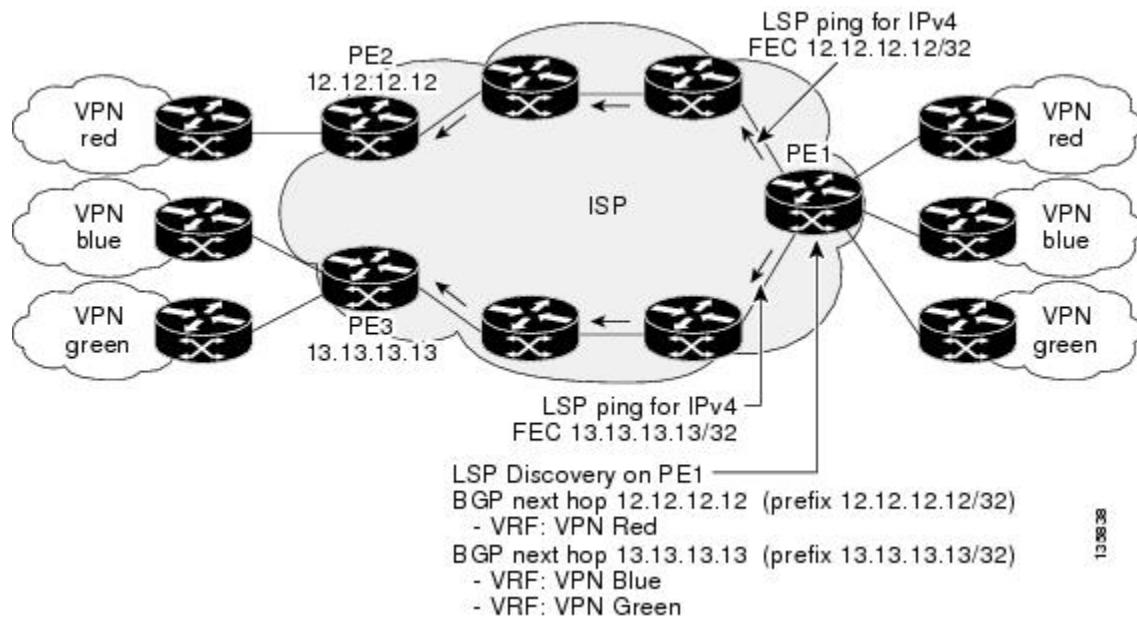
Discovery of Neighboring PE Devices

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

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

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

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



LSP Discovery

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

The general process for LSP discovery is as follows:

1. BGP next hop neighbors are discovered using the BGP next hop neighbor discovery process. For more information about the BGP next hop neighbor discovery process, see the "Discovery of Neighboring PE Routers" section.

Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created for each applicable PE (BGP next hop) neighbor. Only a single path to each applicable PE neighbor is discovered during this initial step of the LSP discovery process. For each next hop neighbor, the LSP Health Monitor creates an LSP discovery group (that initially consists of only the one discovered path) and assigns the group with a unique identification number. For more information about LSP discovery groups, see the "LSP Discovery Groups" section.

2. An LSP discovery request is sent by the LSP Health Monitor to the LSP discovery subsystem for each applicable BGP next hop neighbor. For each next hop neighbor in which an appropriate response is received, MPLS echo requests are sent one-by-one from the source PE device to discover the equal-cost multipaths. The parameters that uniquely identify each equal-cost multipath (127/8 destination IP address [LSP selector] and the PE outgoing interface) are added to the associated LSP discovery database.



Note

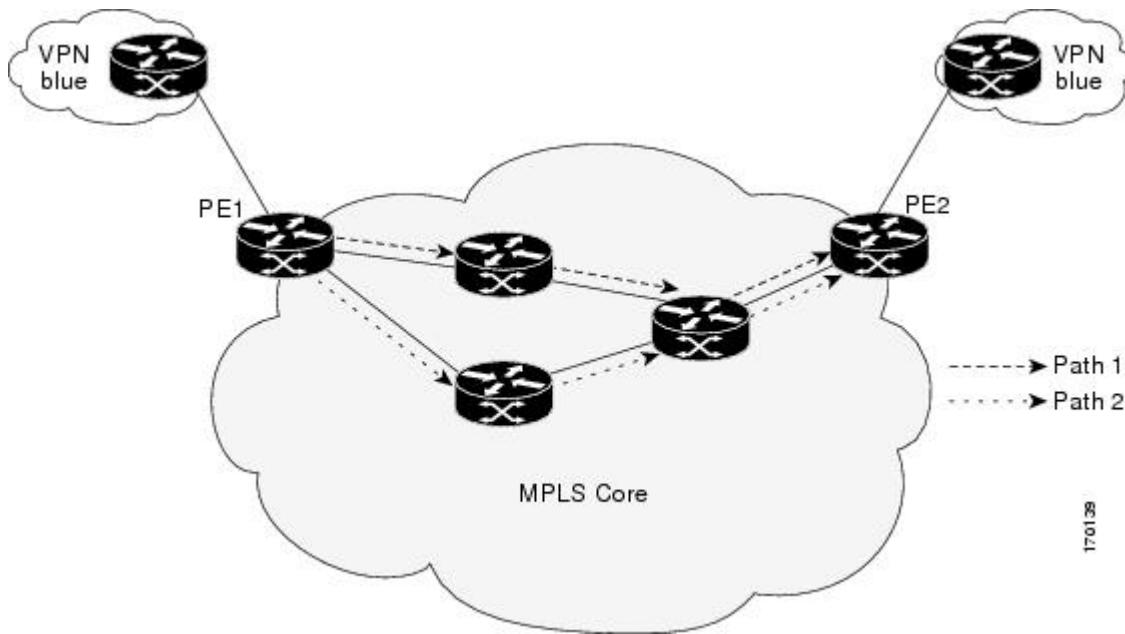
For a given LSP Health Monitor operation, the user can define the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery.

LSP Discovery Groups

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

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

Figure 5: LSP Discovery for a Simple VPN

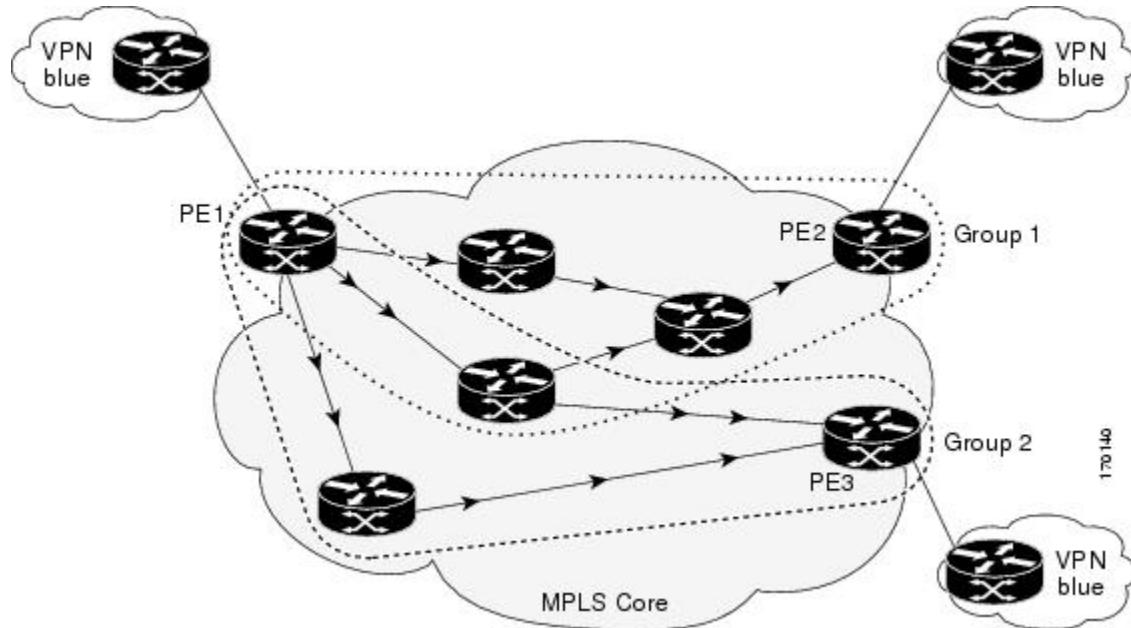


LSP Discovery Groups

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

to device PE2 and LSP discovery group 2 is created for the equal-cost multipaths between device PE1 to device PE3.

Figure 6: LSP Discovery Groups for a Simple VPN



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

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

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

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

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

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

IP SLAs LSP Ping and LSP Traceroute

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

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

The LSP discovery does not support IP SLAs traceroute operations.

Proactive Threshold Monitoring for the LSP Health Monitor

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

LSP Discovery Option Enabled

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

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

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

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

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

Table 12: 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 an LSP Health Monitor

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

Newly created IP SLAs operations (for newly discovered BGP next hop neighbors) are added to the same schedule period as the operations that are currently running. To prevent too many operations from starting at

the same time, the multioperation scheduling feature will schedule the operations to begin at random intervals uniformly distributed over the schedule period.

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

LSP Discovery Enabled

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

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

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

How to Configure LSP Health Monitor Operations

Configuring an LSP Health Monitor Operation

Perform only one of the following tasks:

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



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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval *seconds***
5. **auto ip sla mpls-lsp-monitor *operation-number***
6. Do one of the following:
 - type **echo [ipsla-vrf-all | vrf *vpn-name*]**

- **type pathEcho [ipsla-vrf-all | vrf *vpn-name*]**
- 7. **access-list *access-list-number***
- 8. **scan-interval *minutes***
- 9. **delete-scan-factor *factor***
- 10. **force-explicit-null**
- 11. **exp *exp-bits***
- 12. **lsp-selector *ip-address***
- 13. **reply-dscp-bits *dscp-value***
- 14. **reply-mode {ipv4 | router-alert}**
- 15. **request-data-size *bytes***
- 16. **secondary-frequency {both | connection-loss | timeout} *frequency***
- 17. **tag *text***
- 18. **threshold *milliseconds***
- 19. **timeout *milliseconds***
- 20. **ttl *time-to-live***
- 21. **exit**
- 22. **auto ip sla mpls-lsp-monitor reaction-configuration *operation-number* react {connectionLoss | timeout} [action-type *option*] [threshold-type {consecutive [*occurrences*] | immediate | never}]**
- 23. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	mpls discovery vpn next-hop Example: Device(config)# mpls discovery vpn next-hop	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process. Note This command is automatically enabled when the auto ip sla mpls-lsp-monitor command is entered.
Step 4	mpls discovery vpn interval <i>seconds</i> Example: Device(config)# mpls discovery vpn interval 120	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
Step 5	auto ip sla mpls-lsp-monitor <i>operation-number</i> Example:	Begins configuration for an LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.

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

	Command or Action	Purpose
	Device(config)# auto ip sla mpls-lsp-monitor 1	Note Entering this command automatically enables the mpls discovery vpn next-hop command.
Step 6	<p>Do one of the following:</p> <ul style="list-style-type: none"> • type echo [ipsla-vrf-all vrf <i>vpn-name</i>] • type pathEcho [ipsla-vrf-all vrf <i>vpn-name</i>] <p>Example:</p> <pre>Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all</pre> <p>Example:</p> <pre>Device(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all</pre>	<p>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.</p> <p>or</p> <p>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.</p>
Step 7	access-list <i>access-list-number</i>	(Optional) Specifies the access list to apply to an LSP Health Monitor operation.
Step 8	scan-interval <i>minutes</i>	(Optional) Sets the timer for the IP SLAs LSP Health Monitor database.
Step 9	delete-scan-factor <i>factor</i>	<p>(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.</p> <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	(Optional) Adds an explicit null label to all echo request packets of an IP SLAs operation.

	Command or Action	Purpose
Step 11	exp <i>exp-bits</i> Example: Device(config-auto-ip-sla-mpls-params) # exp 5	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.
Step 12	lsp-selector <i>ip-address</i> Example: Device(config-auto-ip-sla-mpls-params) # lsp-selector 127.0.0.10	(Optional) Specifies the local host IP address used to select the LSP of an IP SLAs operation.
Step 13	reply-dscp-bits <i>dscp-value</i> Example: Device(config-auto-ip-sla-mpls-params) # reply-dscp-bits 5	(Optional) Specifies the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation.
Step 14	reply-mode {ipv4 router-alert} Example: Device(config-auto-ip-sla-mpls-params) # reply-mode router-alert	(Optional) Specifies the reply mode for an echo request packet of an IP SLAs operation. <ul style="list-style-type: none">• The default reply mode is an IPv4 UDP packet.
Step 15	request-data-size <i>bytes</i> Example: Device(config-auto-ip-sla-mpls-params) # request-data-size 200	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
Step 16	secondary-frequency {both connection-loss timeout} <i>frequency</i> Example: Device(config-auto-ip-sla-mpls-params) # secondary-frequency connection-loss 10	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.
Step 17	tag <i>text</i> Example: Device(config-auto-ip-sla-mpls-params) # tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	threshold <i>milliseconds</i> Example: Device(config-auto-ip-sla-mpls-params) # threshold 6000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

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

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

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



Note

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

SUMMARY STEPS

- enable
- configure terminal

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	mpls discovery vpn next-hop Example: <pre>Device(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 <i>seconds</i> Example: <pre>Device(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.

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

	Command or Action	Purpose
Step 5	auto ip sla mpls-lsp-monitor <i>operation-number</i> Example: Device(config)# auto ip sla mpls-lsp-monitor 1	Begins configuration for an LSP Health Monitor operation and enters auto IP SLAs MPLS configuration mode. Note Entering this command automatically enables the mpls discovery vpn next-hop command.
Step 6	type echo [ipsla-vrf-all vrf <i>vpn-name</i>] Example: Device(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all	Enters MPLS parameters configuration mode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.
Step 7	Configure optional parameters for the IP SLAs LSP echo operation.	(Optional) See Steps 7 through 21 in the "Configuring an LSP Health Monitor Operation Without LSP Discovery on a PE Device" section.
Step 8	path-discover Example: Device(config-auto-ip-sla-mpls-params)# path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters LSP discovery parameters configuration submode.
Step 9	hours-of-statistics-kept <i>hours</i> Example: Device(config-auto-ip-sla-mpls-lpd-params)# hours-of-statistics-kept 1	(Optional) Sets the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.
Step 10	force-explicit-null Example: Device(config-auto-ip-sla-mpls-lpd-params)# force-explicit-null	(Optional) Adds an explicit null label to all echo request packets of an LSP Health Monitor operation.
Step 11	interval <i>milliseconds</i> Example: Device(config-auto-ip-sla-mpls-lpd-params)# interval 2	(Optional) Specifies the time interval between MPLS echo requests that are sent as part of the LSP discovery process for an LSP Health Monitor operation.
Step 12	lsp-selector-base <i>ip-address</i> Example: Device(config-auto-ip-sla-mpls-lpd-params)# lsp-selector-base 127.0.0.2	(Optional) Specifies the base IP address used to select the LSPs belonging to the LSP discovery groups of an LSP Health Monitor operation.

	Command or Action	Purpose
Step 13	maximum-sessions <i>number</i> Example: Device(config-auto-ip-sla-mpls-lpd-params) # maximum-sessions 2	(Optional) Specifies the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation. Note Careful consideration should be used when configuring this parameter to avoid a negative impact on the device's CPU.
Step 14	scan-period <i>minutes</i> Example: Device(config-auto-ip-sla-mpls-lpd-params) # scan-period 30	(Optional) Sets the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.
Step 15	session-timeout <i>seconds</i> Example: Device(config-auto-ip-sla-mpls-lpd-params) # session-timeout 60	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its LSP discovery request for a particular BGP next hop neighbor.
Step 16	timeout <i>seconds</i> Example: Device(config-auto-ip-sla-mpls-lpd-params) # timeout 4	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its echo request packets. Note Careful consideration should be used when configuring this parameter to avoid a negative impact on the device's CPU.
Step 17	exit Example: Device(config-auto-ip-sla-mpls-lpd-params) # exit	Exits LSP discovery parameters configuration submode and returns to MPLS parameters configuration mode.
Step 18	exit Example: Device(config-auto-ip-sla-mpls-params) # exit	Exits MPLS parameters configuration mode and returns to global configuration mode.
Step 19	auto ip sla mpls-lsp-monitor reaction-configuration operation-number react lpd {lpd-group [retry <i>number</i>] tree-trace} [action-type trapOnly] Example: Device(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type trapOnly	(Optional) Configures the proactive threshold monitoring parameters for an LSP Health Monitor operation with LSP discovery enabled.
Step 20	ip sla logging traps Example:	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.

Scheduling LSP Health Monitor Operations

	Command or Action	Purpose
	Device(config)# ip sla logging traps	
Step 21	exit Example: <pre>Device(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.

Scheduling LSP Health Monitor Operations

**Note**

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

Before you begin

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

SUMMARY STEPS

- enable**
- configure terminal**
- 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}]**
- exit**
- show ip sla configuration**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<pre>auto ip sla mpls-lsp-monitor schedule <i>operation-number</i> schedule-period <i>seconds</i> [frequency [<i>seconds</i>]] [start-time {after hh:mm:ss hh:mm[:ss] [month day] day month} now pending}]</pre> <p>Example:</p> <pre>Device(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now</pre>	Configures the scheduling parameters for an LSP Health Monitor operation.
Step 4	exit <p>Example:</p> <pre>Device(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5	show ip sla configuration <p>Example:</p> <pre>Device# show ip sla configuration</pre>	(Optional) Displays the IP SLAs configuration details.

Troubleshooting Tips

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

What to Do Next

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. Do one of the following:
 - **mpls lsp ping ipv4 *destination-address* *destination-mask* [force-explicit-null] [lsp-selector *ip-address*] [*src-ip-addr* *source-address*] [reply {dscp *dscp-value* | mode {ipv4 | router-alert}}}}**
 - **mpls lsp trace ipv4 *destination-address* *destination-mask* [force-explicit-null] [lsp-selector *ip-address*] [*src-ip-addr* *source-address*] [reply {dscp *dscp-value* | mode {ipv4 | router-alert}}]}**
5. **exp *exp-bits***

6. **request-data-size bytes**
7. **secondary-frequency {connection-loss | timeout} frequency**
8. **tag text**
9. **threshold milliseconds**
10. **timeout milliseconds**
11. **ttl time-to-live**
12. **exit**
13. **ip sla reaction-configuration operation-number [react monitored-element] [threshold-type {never | immediate | consecutive [consecutive-occurrences] | xofy [x-value y-value] | average [number-of-probes]}] [threshold-value upper-threshold lower-threshold] [action-type {none | trapOnly | triggerOnly | trapAndTrigger}]**
14. **ip sla logging traps**
15. **ip sla schedule operation-number [life {forever | seconds}] [start-time {hh : mm[: ss]} [month day | day month] | pending | now | after hh : mm : ss}] [ageout seconds] [recurring]**
16. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config)# ip sla 1</pre>	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: <pre>Device(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1</pre>	<ul style="list-style-type: none"> The first example configures the IP SLAs operation as an LSP ping operation and enters LSP ping configuration mode. The second example configures the IP SLAs operation as an LSP trace operation and enters LSP trace configuration mode.

	Command or Action	Purpose
	Example: Device(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1	
Step 5	exp exp-bits Example: Device(config-sla-monitor-lspPing)# exp 5	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation. Note The LSP ping configuration mode is used in this example and in the remaining steps. Except where noted, the same commands are also supported in the LSP trace configuration mode.
Step 6	request-data-size bytes Example: Device(config-sla-monitor-lspPing)# request-data-size 200	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
Step 7	secondary-frequency {connection-loss timeout} frequency Example: Device(config-sla-monitor-lspPing)# secondary-frequency connection-loss 10	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs. • This command is for IP SLAs LSP ping operations only. LSP trace configuration mode does not support this command.
Step 8	tag text Example: Device(config-sla-monitor-lspPing)# tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	threshold milliseconds Example: Device(config-sla-monitor-lspPing)# threshold 6000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 10	timeout milliseconds Example: Device(config-sla-monitor-lspPing)# timeout 7000	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
Step 11	ttl time-to-live Example: Device(config-sla-monitor-lspPing)# ttl 200	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.
Step 12	exit Example:	Exits LSP ping or LSP trace configuration submode and returns to global configuration mode.

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

Troubleshooting Tips

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

What to Do Next

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

Verifying and Troubleshooting LSP Health Monitor Operations

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	debug ip sla error [operation-number] Example: Device# debug ip sla error	(Optional) Enables debugging output of IP SLAs operation run-time errors.
Step 2	debug ip sla mpls-lsp-monitor [operation-number] Example: Device# debug ip sla mpls-lsp-monitor	(Optional) Enables debugging output of LSP Health Monitor operations.
Step 3	debug ip sla trace [operation-number] Example: Device# debug ip sla trace	(Optional) Enables debugging output for tracing the execution of IP SLAs operations.
Step 4	show ip sla mpls-lsp-monitor collection-statistics [group-id] Example: Device# show ip sla mpls-lsp-monitor collection-statistics 100001	(Optional) Displays the statistics for IP SLAs operations belonging to an LSP discovery group of an LSP Health Monitor operation. Note This command is applicable only if the LSP discovery option is enabled.
Step 5	show ip sla mpls-lsp-monitor configuration [operation-number] Example: Device# show ip sla mpls-lsp-monitor configuration 1	(Optional) Displays configuration settings for LSP Health Monitor operations.

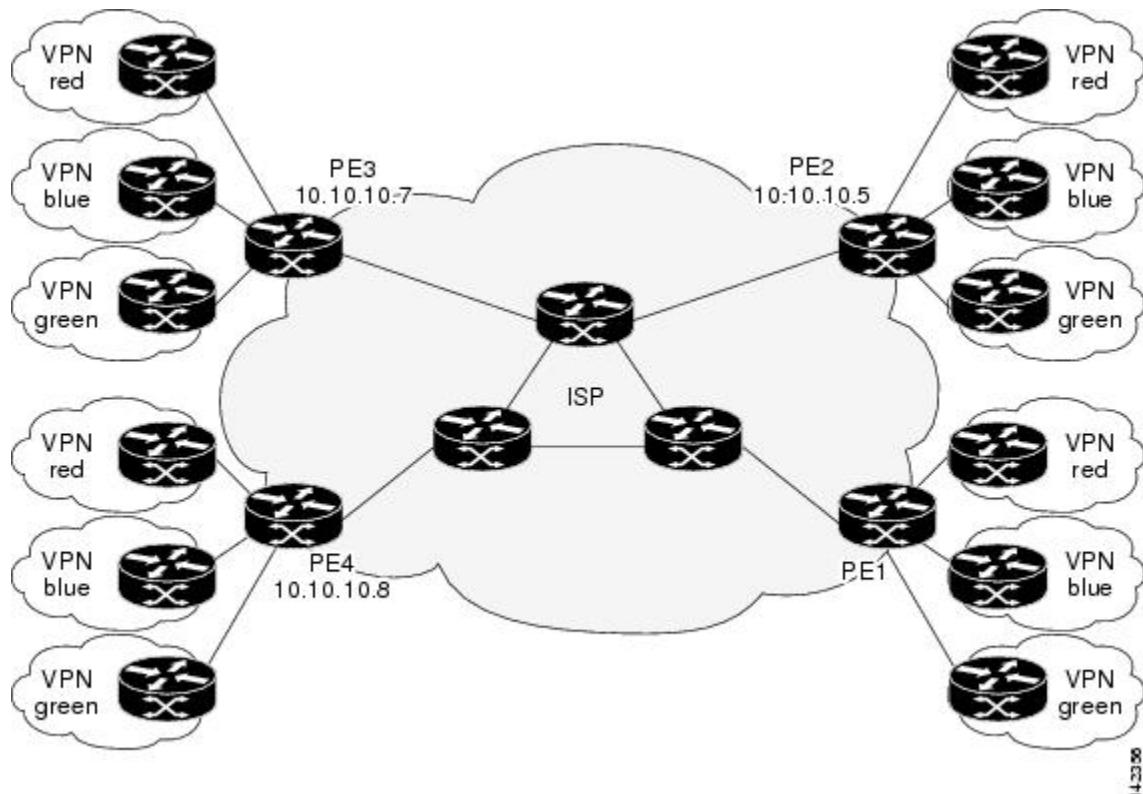
	Command or Action	Purpose
Step 6	show ip sla mpls-lsp-monitor lpd operational-state [group-id] Example: Device# show ip sla mpls-lsp-monitor lpd operational-state 100001	(Optional) Displays the operational status of the LSP discovery groups belonging to an LSP Health Monitor operation. Note This command is applicable only if the LSP discovery option is enabled.
Step 7	show ip sla mpls-lsp-monitor neighbors Example: Device# show ip sla mpls-lsp-monitor neighbors	(Optional) Displays routing and connectivity information about MPLS VPN BGP next hop neighbors discovered by the LSP Health Monitor operation.
Step 8	show ip sla mpls-lsp-monitor scan-queue operation-number Example: Device# show ip sla mpls-lsp-monitor scan-queue 1	(Optional) Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an LSP Health Monitor operation.
Step 9	show ip sla mpls-lsp-monitor summary [operation-number [group [group-id]]] Example: Device# show ip sla mpls-lsp-monitor summary	(Optional) Displays BGP next hop neighbor and LSP discovery group information for LSP Health Monitor operations. Note This command is applicable only if the LSP discovery option is enabled.
Step 10	show ip sla statistics [operation-number] [details] Example: Device# show ip sla statistics 100001	(Optional) Displays the current operational status and statistics of all IP SLAs operations or a specified operation. Note This command applies only to manually configured IP SLAs operations.
Step 11	show ip sla statistics aggregated [operation-number] [details] Example: Device# show ip sla statistics aggregated 100001	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation. Note This command applies only to manually configured IP SLAs operations.
Step 12	show mpls discovery vpn Example: Device# show mpls discovery vpn	(Optional) Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

Configuration Examples for LSP Health Monitors

Example Configuring and Verifying the LSP Health Monitor Without LSP Discovery

The figure below illustrates a simple VPN scenario for an ISP. This network consists of a core MPLS VPN with four PE devices belonging to three VPNs: red, blue, and green. From the perspective of device PE1, these VPNs are reachable remotely through BGP next hop devices PE2 (device ID: 10.10.10.5), PE3 (device ID: 10.10.10.7), and PE4 (device ID: 10.10.10.8).

Figure 7: Network Used for LSP Health Monitor Example



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

Example Configuring and Verifying the LSP Health Monitor Without LSP Discovery

occur, an SNMP trap notification is sent. Multioperation scheduling and the generation of IP SLAs SNMP system logging messages are enabled.

PE1 Configuration

```

mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
  type echo ipsla-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency both 10
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3 action-type trapOnly
ip sla traps
snmp-server enable traps rtr
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

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

```

PE1# show ip sla mpls-lsp-monitor configuration 1
Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type    : echo
Vrf Name          : ipsla-vrf-all
Tag               :
EXP Value         : 0
Timeout(ms)       : 1000
Threshold(ms)     : 5000
Frequency(sec)    : Equals schedule period
LSP Selector      : 127.0.0.1
ScanInterval(min) : 1
Delete Scan Factor: 1
Operations List   : 1000001-100003
Schedule Period(sec): 60
Request size      : 100
Start Time        : Start Time already passed
SNMP RowStatus    : Active
TTL value         : 255
Reply Mode        : ipv4
Reply Dscp Bits  :
Secondary Frequency: Enabled on Timeout
Value(sec)         : 10
Reaction Configs  :
  Reaction        : connectionLoss
  Threshold Type  : Consecutive
  Threshold Count : 3
  Action Type     : Trap Only
  Reaction        : timeout
  Threshold Type  : Consecutive
  Threshold Count : 3
  Action Type     : Trap Only

```

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

```
PE1# show mpls discovery vpn
```

```

Refresh interval set to 60 seconds.
Next refresh in 46 seconds
Next hop 10.10.10.5 (Prefix: 10.10.10.5/32)
    in use by: red, blue, green
Next hop 10.10.10.7 (Prefix: 10.10.10.7/32)
    in use by: red, blue, green
Next hop 10.10.10.8 (Prefix: 10.10.10.8/32)
    in use by: red, blue, green

```

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

```

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

```

The following is sample output from the **show ip sla mpls-lsp-monitor scan-queue 1** and **debug ip sla mpls-lsp-monitor** commands when IP connectivity from PE1 to PE4 is lost. This output shows that connection loss to each of the VPNs associated with PE4 (red, blue, and green) was detected and that this information was added to the LSP Health Monitor scan queue. Also, since PE4 is no longer a valid BGP next hop neighbor, the IP SLAs operation for PE4 (Probe 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 PE1 to PE4 is restored. This output shows that each of the VPNs associated with PE4 (red, blue, and green) were discovered and that this information was added to the LSP Health Monitor scan queue. Also, since PE4 is a newly discovered BGP next hop neighbor, a new IP SLAs operation for PE4 (Probe 100005) is being created and added to the LSP Health Monitor multioperation schedule. Even though PE4 belongs to three VPNs, only one IP SLAs operation is being created.

```

PE1# show ip sla mpls-lsp-monitor scan-queue 1
Next scan Time after: 23 Secs
Next Delete scan Time after: 23 Secs
BGP Next hop      Prefix          vrf          Add/Delete?
10.10.10.8        10.10.10.8/32  red          Add
10.10.10.8        10.10.10.8/32  blue         Add
10.10.10.8        10.10.10.8/32  green        Add
PE1# debug ip sla mpls-lsp-monitor
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ

```

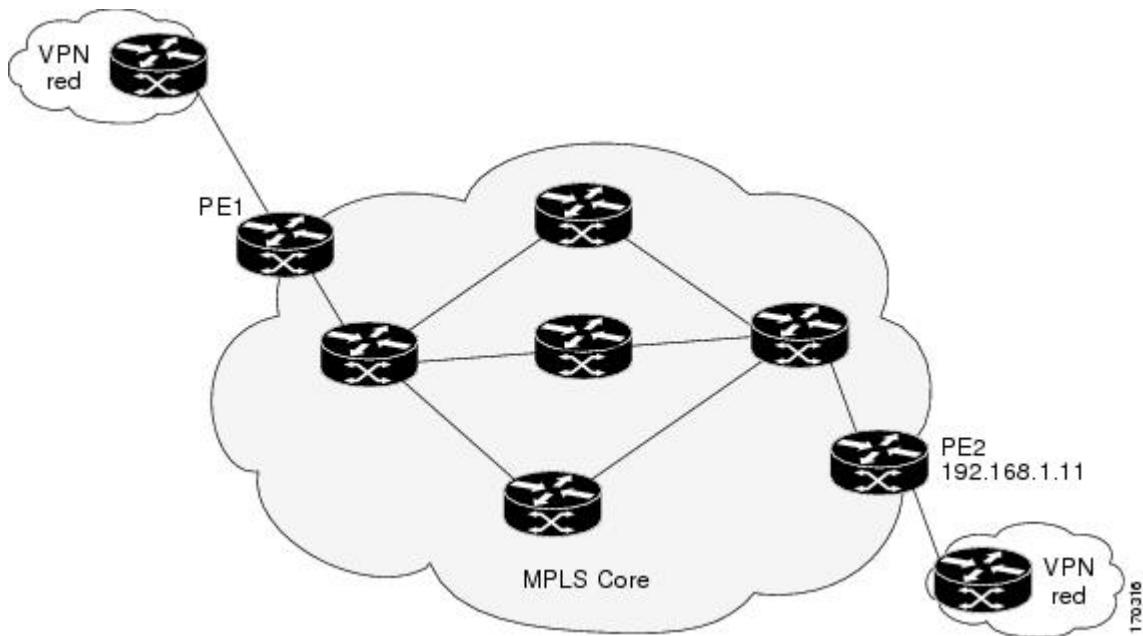
Example Configuring and Verifying the LSP Health Monitor with LSP Discovery

```
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf red into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding Probe 100005
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding ProbeID 100005 to tree entry 10.10.10.8 (1)
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf blue into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf green into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Added Probe(s) 100005 will be scheduled after 26 secs over
schedule period 60
```

Example Configuring and Verifying the LSP Health Monitor with LSP Discovery

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

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



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

PE1 Configuration

```

mpls discovery vpn next-hop
mpls discovery vpn interval 30
!
auto ip sla mpls-lsp-monitor 100
  type echo ipsla-vrf-all
  scan-interval 1
  secondary-frequency both 5
!
path-discover
force-explicit-null
scan-period 3
!
auto ip sla mpls-lsp-monitor reaction-configuration 100 react lpd-group retry 3 action-type
  trapOnly
!
auto ip sla mpls-lsp-monitor schedule 100 schedule-period 30 start-time now
!
ip sla logging traps
snmp-server enable traps rtr

```

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

```

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

```

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

Example Configuring and Verifying the LSP Health Monitor with LSP Discovery

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

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

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

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

```
PE1# show ip sla mpls-lsp-monitor lpd operational-state
Entry number: 100001
MPLSLM Entry Number: 100
Target FEC Type: LDP IPv4 prefix
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :
  Path Outgoing Lsp           Link Conn Adj      Downstream
  Index Interface Selector   Type Id   Addr      Label Stack Status
  1     Et0/0    127.0.0.8    90    0    10.10.18.30  21          OK
  2     Et0/0    127.0.0.2    90    0    10.10.18.30  21          OK
  3     Et0/0    127.0.0.1    90    0    10.10.18.30  21          OK
```

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

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

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

```
PE1# show ip sla mpls-lsp-monitor summary 100
```

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

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

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

Example Manually Configuring an IP SLAs LSP Ping Operation

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

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

Additional References

Related Documents

Related Topic	Document Title
MPLS LSP discovery management tool	"MPLS EM-MPLS LSP Multipath Tree Trace" chapter of the <i>Multiprotocol Label Switching Configuration Guide</i>
Configuring standard IP access lists	"Access Control Lists" chapter of the <i>Security Configuration Guide: Securing the Data Plane</i> guide

Additional References

Related Topic	Document Title
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" chapter of the <i>Cisco IOS P SLAs Configuration Guide</i>
Proactive threshold monitoring for 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	Cisco IOS IP SLAs Command Reference

Standards

Standard	Title
draft-ietf-mpls-lsp-ping-09.txt	Detecting MPLS Data Plane Failures
draft-ietf-mpls-oam-frmwk-03.txt	A Framework for MPLS Operations and Management (OAM)
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 13: Feature Information for the LSP Health Monitor

Feature Name	Releases	Feature Information
IP SLAs--LSP Health Monitor	12.2(27)SBC 12.2(28)SB 12.2(33)SRA 12.4(6)T 15.0(1)SY 15.0(1)S 12.2(50)SY	The IP SLAs LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs.
IP SLAs--LSP Health Monitor	12.2(31)SB2 12.2(33)SB 12.2(33)SRB 12.2(33)SXH	For software releases in which this feature was already introduced, new command-line interface (CLI) was implemented that replaces the CLI introduced in the earlier releases
IP SLAs--LSP Health Monitor with LSP Discovery	12.2(31)SB2 12.2(33)SRB 15.0(1)S 12.2(50)SY 15.4(1)S	The LSP discovery capability was added. In Cisco IOS Release 15.4(1)S, support was added for the Cisco ASR 901S Router.



CHAPTER 6

IP SLAs for MPLS Pseudo Wire via VCCV

This module describes how to configure IP Service Level Agreements (SLAs) for MPLS Pseudo Wire (PWE3) via Virtual Circuit Connectivity Verification (VCCV) to schedule pseudo-wire ping operations and provide monitoring and alerts for round trip time (RTT), failure, and connection threshold violations via SNMP Traps.

- [Finding Feature Information, on page 93](#)
- [Restrictions for IP SLAs for MPLS Pseudo Wire via VCCV, on page 93](#)
- [Information About IP SLAs for MPLS Pseudo Wire via VCCV, on page 93](#)
- [How to Configure IP SLAs for MPLS Pseudo Wire via VCCM, on page 95](#)
- [Configuration Examples for IP SLAs for MPLS Pseudo Wire via VCCM, on page 98](#)
- [Additional References, on page 99](#)
- [Feature Information for IP SLAs for MPLS PWE3 via VCCM, on page 101](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs for MPLS Pseudo Wire via VCCV

LSP discovery is not supported for IP SLAs VCCV operations.

Information About IP SLAs for MPLS Pseudo Wire via VCCV

IP SLAs VCCV Operation

The IP SLAs VCCV operation supports Virtual Circuit Connectivity Verification (VCCV) for Pseudo-Wire Emulation Edge-to-Edge (PWE3) services across MPLS networks. The IP SLAs VCCV operation type is

based on the **ping mpls pseudowire** command, which checks MPLS LSP connectivity across an Any Transport over MPLS (AToM) virtual circuit (VC) by sending a series of pseudo-wire ping operations to the specified destination PE router.

When MPLS LSP connectivity checking is performed through an IP SLAs VCCV operation (rather than through the **ping mpls** command with the **pseudowire** keyword), you can use the IP SLA proactive threshold monitoring and multioperation scheduling capabilities:

The LSP discovery option does not support the IP SLAs VCCV operation.

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 14: Conditions for Which an LSP Discovery Group Status Changes

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

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

- OK--Indicates that the LSP is working properly. The customer VPN traffic will be sent across this path.

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

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

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

Secondary Frequency Option

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

How to Configure IP SLAs for MPLS Pseudo Wire via VCCM

Manually Configuring and Scheduling an IP SLAs VCCV Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **mpls lsp ping pseudowire *peer-ipaddr vc-id* [**source-ipaddr source-ipaddr**]**
5. **exp *exp-bits***
6. **frequency *seconds***
7. **request-data-size *bytes***
8. **secondary-frequency {both | connection-loss | timeout} *frequency***
9. **tag *text***
10. **threshold *milliseconds***
11. **timeout *milliseconds***
12. **exit**

Manually Configuring and Scheduling an IP SLAs VCCV Operation

13. **ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value* *y-value*] | **average** [*number-of-probes*] }] [**threshold-value** *upper-threshold* *lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]
14. **ip sla logging traps**
15. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh : mm[: ss]*} [*month day* | *day month*] | **pending** | **now** | **after** *hh : mm : ss*] [**ageout** *seconds*] [**recurring**]
16. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <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 <i>operation-number</i> Example: <pre>Router(config)# ip sla 777</pre>	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	mpls lsp ping pseudowire <i>peer-ipaddr vc-id</i> [source-ipaddr <i>source-ipaddr</i>] Example: <pre>Router(config-ip-sla)# mpls lsp ping pseudowire 192.168.1.103 123 source-ipaddr 192.168.1.102</pre>	Configures the IP SLAs operation as an LSP pseudo-wire ping and enters VCCV configuration mode.
Step 5	exp <i>exp-bits</i> Example: Example: <pre>Router(config-sla-vccv)# exp 5</pre>	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.
Step 6	frequency <i>seconds</i> Example: <pre>Router(config-sla-vccv)# frequency 120</pre>	(Optional) Specifies the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 7	request-data-size bytes Example: Router(config-sla-vccv)# request-data-size 200	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
Step 8	secondary-frequency {both connection-loss timeout} frequency Example: Router(config-sla-vccv)# secondary-frequency connection-loss 10	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.
Step 9	tag text Example: Router(config-sla-vccv)# tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 10	threshold milliseconds Example: Example: Router(config-sla-vccv)# threshold 6000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 11	timeout milliseconds Example: Router(config-sla-vccv)# timeout 7000	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
Step 12	exit Example: Router(config-sla-vccv)# exit	Exits VCCV configuration mode and returns to global configuration mode.
Step 13	ip sla reaction-configuration operation-number [react monitored-element] [threshold-type {never immediate consecutive [consecutive-occurrences]} xofy [x-value y-value] average [number-of-probes]]] [threshold-value upper-threshold lower-threshold] [action-type {none trapOnly triggerOnly trapAndTrigger}] Example: Router(config)# ip sla reaction-configuration 777 react connectionLoss threshold-type consecutive 3 action-type traponly	(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.

	Command or Action	Purpose
Step 14	ip sla logging traps Example: Router(config)# ip sla logging traps	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
Step 15	ip sla schedule operation-number [life {forever seconds}] [start-time {hh : mm[: ss] [month day day month} pending now after hh : mm : ss}] [ageout seconds] [recurring] Example: Router(config)# ip sla schedule 777 life forever start-time now	Configures the scheduling parameters for an IP SLAs operation.
Step 16	exit Example: Router(config)# exit	Exits global configuration submode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs PWE3 service via VCCV 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.

Configuration Examples for IP SLAs for MPLS Pseudo Wire via VCCM

Example Manually Configuring an IP SLAs VCCV Operation

The following example shows how to manually configure an IP SLAs VCCV operation in conjunction with the proactive threshold monitoring and multioperation scheduling capabilities of the LSP Health Monitor.

In this example, a VC with the identifier 123 has already been established between the PE device and its peer at IP address 192.168.1.103.

IP SLAs VCCV operation 777 is configured with operation parameters and reaction conditions, and it is scheduled to begin immediately and run indefinitely.

```
ip sla 777
  mpls lsp ping pseudowire 192.168.1.103 123
```

```

exp 5
frequency 120
secondary-frequency timeout 30
tag testgroup
threshold 6000
timeout 7000
exit
!
ip sla reaction-configuration 777 react rtt threshold-value 6000 3000 threshold-type
immediate 3 action-type traponly
ip sla reaction-configuration 777 react connectionLoss threshold-type immediate action-type
traponly
ip sla reaction-configuration 777 react timeout threshold-type consecutive 3 action-type
traponly
ip sla logging traps
!
ip sla schedule 777 life forever start-time now
exit

```

RTT Thresholds

The **threshold** command configures 6000 milliseconds as the amount of time for a rising threshold to be declared on the monitored pseudo-wire. The first **ip sla reaction-configuration** command specifies that an SNMP logging trap is to be sent immediately if the round-trip time violates the upper threshold of 6000 milliseconds or the lower threshold of 3000 milliseconds.

Connection Loss

The second **ip sla reaction-configuration** command specifies that an SNMP logging trap is to be sent immediately if a connection loss occurs for the monitored pseudo-wire.

Response Timeout

The **timeout** command configures 7000 seconds as the amount of time that VCCV operation 777 waits for a response from its request packet before a timeout is declared. The **secondary-frequency** command specifies that, if a timeout occurs, the measurement frequency of the operation repeats is to be increased from 120 seconds (the initial measurement frequency specified using the **frequency** command) to a faster rate of 30 seconds. The third **ip sla reaction-configuration** command specifies that an SNMP logging trap is to be sent if three consecutive timeouts occur.

Additional References

Related Documents

Related Topic	Document Title
MPLS LSP discovery management tool	"MPLS EM-MPLS LSP Multipath Tree Trace" chapter of the <i>Multiprotocol Label Switching Configuration Guide</i>
Configuring standard IP access lists	"Access Control Lists" chapter of the <i>Security Configuration Guide: Securing the Data Plane</i> guide
Multioperation scheduling for IP SLAs	"Configuring Multioperation Scheduling of IP SLAs Operations" chapter of the <i>Cisco IOS P SLAs Configuration Guide</i>

Additional References

Related Topic	Document Title
Proactive threshold monitoring for 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	Cisco IOS IP SLAs Command Reference

Standards

Standard	Title
draft-ietf-mpls-lsp-ping-09.txt	Detecting MPLS Data Plane Failures
draft-ietf-mpls-oam-frmwk-03.txt	A Framework for MPLS Operations and Management (OAM)
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 IP SLAs for MPLS PWE3 via VCCM

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: IP SLAs for MPLS PWE3 via VCCM

Feature Name	Releases	Feature Information
IP SLAs for MPLS Pseudo Wire (PWE3) via VCCM	12(33)SB 12.2(33)SRC 15.0(1)S Cisco IOS XE 3.1.0SG	The IP SLAs VCCV operation was added to support Virtual Circuit Connectivity Verification (VCCV) for Pseudo-Wire Emulation Edge-to-Edge (PWE3) services across MPLS networks.



CHAPTER 7

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, on page 103](#)
- [Prerequisites for IP SLAs for Metro-Ethernet, on page 103](#)
- [Restrictions for IP SLAs for Metro-Ethernet, on page 103](#)
- [Information About IP SLAs for Metro-Ethernet, on page 104](#)
- [How to Configure IP SLAs for Metro-Ethernet, on page 105](#)
- [Configuration Examples for IP SLAs for Metro-Ethernet, on page 112](#)
- [Additional References, on page 113](#)
- [Feature Information for IP SLAs for Metro-Ethernet, on page 114](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP SLAs for Metro-Ethernet

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

Restrictions for IP SLAs for Metro-Ethernet

- Memory and performance may be impacted for a given Ethernet CFM maintenance domain and Ethernet Virtual Circuit (EVC) or VLAN that has a large number of maintenance endpoints (MEPs).

- In case of PW redundancy, we need to have 2 different CFM/Y1731 sessions on active and backup PW. We cannot expect the same mpid and Y1731 session to work after PW switchover.
- Y1731 is not supported for port meps.
- CFM ans Y1731 is not supported for vpls cases, untagged EFP as well.

Information About IP SLAs for Metro-Ethernet

IP SLAs Ethernet Operation Basics

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

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

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

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

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

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

Statistics Measured by the IP SLAs Ethernet Operation

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

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

How to Configure IP SLAs for Metro-Ethernet

**Note**

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla ethernet-monitor *operation-number***
4. **type echo domain *domain-name* {evc *evc-id* | vlan *vlan-id*} [exclude-mpids *mp-ids*]**
5. **type jitter domain *domain-name* {evc *evc-id* | vlan *vlan-id*} [exclude-mpids *mp-ids*] [interval *interframe-interval*] [**num-frames** *frames-number*]**
6. **cos *cos-value***
7. **owner *owner-id***
8. **request-data-size *bytes***
9. **tag *text***
10. **threshold *milliseconds***
11. **timeout *milliseconds***
12. **end**
13. **show ip sla ethernet-monitor configuration [*operation-number*]**

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	type echo domain domain-name {evc evc-id vlan vlan-id} [exclude-mpids mp-ids] Example: <pre>Device(config-ip-sla-ethernet-monitor)# type echo domain testdomain vlan 34</pre>	<ul style="list-style-type: none"> • domain domain-name—Specify the name of the created domain. • vlan vlan-id—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma. • exclude-mpids mp-ids—Enter a maintenance end point identifier (mpid). The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. <p>For Echo operations only: Configures an auto Ethernet operation for Ethernet ping operations.</p> <p>Note Depending on your release, the evc evc-id keyword and argument combination may not be available for this command.</p>
Step 5	type jitter domain domain-name {evc evc-id vlan vlan-id} [exclude-mpids mp-ids] [interval interframe-interval] [num-frames frames-number] Example: <pre>Device(config-ip-sla-ethernet-monitor)# type jitter domain testdomain evc testevc interval 20 num-frames 30</pre>	<p>For Jitter operations only: Configures an auto Ethernet operation for Ethernet jitter operations.</p> <p>Note Depending on your release, the evc evc-id keyword and argument combination may not be available for this command.</p>
Step 6	cos cos-value Example: <pre>Device(config-ip-sla-ethernet-params)# cos 2</pre>	(Optional) Sets the class of service for an IP SLAs Ethernet operation.
Step 7	owner owner-id Example: <pre>Device(config-ip-sla-ethernet-params)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 8	request-data-size bytes Example: <pre>Device(config-ip-sla-ethernet-params)# request-data-size 64</pre>	<p>(Optional) Sets the padding size for the data frame of an IP SLAs Ethernet operation.</p> <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.
Step 9	tag text Example:	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
	Device(config-ip-sla-ethernet-params) # tag TelnetPollServer1	
Step 10	threshold milliseconds Example: Device(config-ip-sla-ethernet-params) # threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 11	timeout milliseconds Example: Device(config-ip-sla-ethernet-params) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 12	end Example: Device(config-ip-sla-ethernet-params) # end	Exits to privileged EXEC configuration mode.
Step 13	show ip sla ethernet-monitor configuration [operation-number] Example: Device# show ip sla ethernet-monitor configuration 1	(Optional) Displays configuration settings for all IP SLAs auto Ethernet operations or a specified auto Ethernet operation.

What to do next

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **ethernet echo mpid mp-id domain domain-name {evc evc-id | port | vlan vlan-id}**
5. **ethernet jitter mpid mp-id domain domain-name {evc evc-id | port | vlan vlan-id} [interval interframe-interval] [num-frames frames-number]**
6. **cos cos-value**
7. **frequency seconds**
8. **history history-parameter**

9. **owner** *owner-id*
10. **request-data-size** *bytes*
11. **tag** *text*
12. **threshold** *milliseconds*
13. **timeout** *milliseconds*
14. **end**
15. **show ip sla configuration** [*operation-number*]
16. **show ip sla application**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 1	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ethernet echo mpid mp-id domain domain-name {evc evc-id port vlan vlan-id} Example: Device(config-ip-sla)# ethernet echo mpid 23 domain testdomain vlan 34	For a ping operation only: Configures the IP SLAs operation as an Ethernet ping operation and enters Ethernet echo configuration mode. Note Depending on your release, the evc evc-id keyword and argument combination may not be available for this command.
Step 5	ethernet jitter mpid mp-id domain domain-name {evc evc-id port vlan vlan-id} [interval interframe-interval] [num-frames frames-number] Example: Device(config-ip-sla)# ethernet jitter mpid 23 domain testdomain evc testevc interval 20 num-frames 30	For a jitter operation only: Configures the IP SLAs operation as an Ethernet jitter operation and enters Ethernet jitter configuration mode. Note Depending on your release, the evc evc-id keyword and argument combination may not be available for this command.
Step 6	cos cos-value Example:	(Optional) Sets the class of service for an IP SLAs Ethernet operation.

	Command or Action	Purpose
	Device(config-ip-sla-ethernet-echo)# cos 2	Note For this and the remaining steps, the configuration mode shown in the example is for configuring an Ethernet echo operation. However, the commands are the same in the Ethernet jitter configuration mode.
Step 7	frequency seconds Example: Device(config-ip-sla-ethernet-echo)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 8	history history-parameter Example: Device(config-ip-sla-ethernet-echo)# history hours-of-statistics-kept 3	(Optional) Specifies the parameters used for gathering statistical history information for an IP SLAs operation.
Step 9	owner owner-id Example: Device(config-ip-sla-ethernet-echo)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 10	request-data-size bytes Example: Device(config-ip-sla-ethernet-echo)# request-data-size 64	(Optional) Sets the padding size for the data frame of an IP SLAs Ethernet operation. The default value for IP SLAs Ethernet ping operations is 66 bytes. The default value for IP SLAs Ethernet jitter operations is 51 bytes.
Step 11	tag text Example: Device(config-ip-sla-ethernet-echo)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 12	threshold milliseconds Example: Device(config-ip-sla-ethernet-echo)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 13	timeout milliseconds Example: Device(config-ip-sla-ethernet-echo)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 14	end Example:	Exits to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-ip-sla-ethernet-echo) # end	
Step 15	show ip sla configuration [operation-number] Example: Device# show ip sla configuration 1	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.
Step 16	show ip sla application Example: Device# show ip sla application	(Optional) Displays global information about supported IP SLAs features.

What to do next

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

Scheduling IP SLAs Operations

**Note**

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
 - **ip sla ethernet-monitor schedule operation-number schedule-period seconds [frequency [seconds]] [start-time {after hh : mm : ss | hh : mm[: ss] [month day | day month] | now | pending}]**
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {hh : mm[: ss] [month day | day month] | pending | now | after hh : mm : ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers schedule-period schedule-period-range [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time{hh:mm[:ss]} [month day | day month] | pending | now | after hh:mm:ss}]**
4. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Do one of the following: <ul style="list-style-type: none"> • ip sla ethernet-monitor schedule operation-number schedule-period seconds [frequency [seconds]] [start-time {after hh : mm : ss hh : mm[: ss] [month day day month] now pending}] • ip sla schedule operation-number [life {forever seconds}] [start-time {hh : mm[: ss] [month day day month] pending now after hh : mm : ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers schedule-period schedule-period-range [ageout seconds] frequency group-operation-frequency [life{forever seconds}] [start-time{hh:mm[:ss] [month day day month] pending now after hh:mm:ss}] Example: Device(config)# ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now Device(config)# ip sla schedule 1 start-time now life forever Device(config)# ip sla group schedule 1 3,4,6-9	<ul style="list-style-type: none"> • The first example shows how to configure scheduling parameters for an IP SLAs auto Ethernet operation. • The second example shows how to configure the scheduling parameters for an individual IP SLAs operation. • The third example shows how to specify an IP SLAs operation group number and range of operation numbers to be scheduled for a multioperation scheduler.
Step 4	exit Example: Device(config)# exit	Exits to the privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays the IP SLAs group schedule details.

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

Troubleshooting Tips

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

What to Do Next

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

operation)

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

Configuration Examples for IP SLAs for Metro-Ethernet

Example IP SLAs Auto Ethernet Operation with Endpoint Discovery

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

Configuration A

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

Configuration B

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

Example Individual IP SLAs Ethernet Ping Operation

The following example show the configuration for an IP SLAs Ethernet ping operation. In Configuration C, the maintenance endpoint identification number is 23, the maintenance domain name is testdomain, and the VLAN identification number is 34. In Configuration D, the maintenance endpoint identification number is 23, the maintenance domain name is testdomain, and the EVC is identified as testevc. In both configurations, the proactive threshold monitoring configuration specifies that when three consecutive connection loss events occur, an SNMP trap notification should be sent. Operation 1 and operation 5 are scheduled to start immediately.

Configuration C

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

Configuration D

```
ip sla 5
  ethernet echo mpid 23 domain testdomain evc testevc
!
ip sla reaction-configuration 5 react connectionLoss threshold-type consecutive 3 action-type
trapOnly
!
ip sla schedule 5 start-time now
```

Additional References**Related Documents**

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

Related Topic	Document Title
Multioperation scheduling for IP SLAs	“Configuring Multioperation Scheduling of IP SLAs Operations” module of the <i>Cisco IOS P SLAs Configuration Guide</i>
Proactive threshold monitoring for IP SLAs	“Configuring Proactive Threshold Monitoring of IP SLAs Operations” module of the <i>Cisco IOS IP SLAs Configuration Guide</i>

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs for Metro-Ethernet

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 16: Feature Information for IP SLAs for Metro-Ethernet

Feature Name	Releases	Feature Information
IP SLAs for Metro-Ethernet	12.2(33)SB 12.2(33)SRB 12.2(33)SXI	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.

Feature Name	Releases	Feature Information
IP SLAs Metro-Ethernet 2.0 (EVC)	12.2(33)SRD	Support for Ethernet Virtual Circuits (EVCs) was added.
IP SLAs Metro-Ethernet 3.0 (CFM d8.1)	12.3(33)SRE 15.0(1)S	Support for the Standards Based EOAM Performance Monitoring CFM base feature was added. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 900 Series.



CHAPTER 8

Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

This module describes how to configure an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation to gather the following performance measurements for Ethernet service:

- Ethernet Delay
- Ethernet Delay Variation
- Ethernet Frame Loss Ratio
- [Finding Feature Information, on page 117](#)
- [Prerequisites for ITU-T Y.1731 Operations, on page 117](#)
- [Restrictions for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\), on page 118](#)
- [How to Configure IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations, on page 118](#)
- [Configuration Examples for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations, on page 131](#)
- [Additional References for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations , on page 134](#)
- [Feature Information for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations, on page 135](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for ITU-T Y.1731 Operations

IEEE-compliant Connectivity Fault Management (CFM) must be configured and enabled for Y.1731 performance monitoring to function.



Note Y1731 is supported on Port Channel interfaces.

Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)

- SNMP is not supported for reporting threshold events or collecting performance statistics for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operations.
- SNMP is partially supported; the results for DM/LM can be polled for some attributes. However MIB support for all parameters is not supported.
- Continuity Check Message (CCM)-based dual-ended Ethernet frame loss operations are not supported.
- In a single-ended Ethernet operation, performance measurement statistics can be retrieved only at the device on which the sender Ethernet Connectivity Fault Management (CFM) Maintenance End Point (MEP) is configured.
- To avoid losing the CoS value configured on the frames, do not configure **rewrite** on the EFPs throughout the Layer2 circuit. The CoS value is preserved, if the Y.1731 frames are marked with specific CoS value.
- CFM over cross-connect on the routers works only if the **control-word** is configured. To start DM timestamping, switch ON the control-word if the remote end is not switched ON.
- To avoid errors in RX and TX timestamping, ensure to have Y1731 sender as PTP master, and the Y1731 responder as PTP slave.
- Reconfigure IP SLA Y1731 while doing online insertion removal (OIR) of IM or router reload because local MEP is deleted during the course.
- A delay may be observed after issuing the **ip sla schedule** command after a reload of the router is performed, to populate with the Y.1731 PM measurements.
- The dot1q tag contains class of service (CoS) bits, which are used by IPSLA Y.1731 PM session to test delay or loss of packets with a specific CoS. This CoS cannot be a non-zero value when using EPM over untagged EFPs.

How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Configuring a Dual-Ended Ethernet Delay or Delay Variation Operation

Perform the tasks for configuring a dual-ended operation in the order presented.



Note To remove the MEP configurations in an already-configured dual-ended operation, always remove the MEPs in the reverse order in which they were configured. That is, remove the scheduler first, then the threshold monitoring configuration, and then the sender MEP configuration on the source device before removing the scheduler, proactive threshold monitoring, and receiver MEP configuration on the destination device.

Configuring a Receiver MEP on the Destination Device

Before you begin

Time synchronization is required between the source and destination devices in order to provide accurate one-way delay (latency) or delay-variation measurements. Configure either Precision Time Protocol (PTP) or Network Time Protocol (NTP) on both the source and destination devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **ethernet y1731 delay receive 1DM domain *domain-name* {evc *evc-id* | vlan *vlan-id*} cos *cos* {mpid *source-mp-id* | mac-address *source-address*}**
5. **aggregate interval *seconds***
6. **distribution {delay | delay-variation} one-way *number-of-bins boundary[,...,boundary]***
7. **frame offset *offset-value***
8. **history interval *intervals-stored***
9. **max-delay *milliseconds***
10. **owner *owner-id***
11. **end**

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 <i>operation-number</i> Example: <pre>Router(config-term)# ip sla 501</pre>	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	ethernet y1731 delay receive 1DM domain <i>domain-name</i> {evc <i>evc-id</i> vlan <i>vlan-id</i>} cos <i>cos</i> {mpid <i>source-mp-id</i> mac-address <i>source-address</i>} Example: <pre>Router(config-ip-sla)# ethernet y1731 delay receive 1DM domain xxx evc yyy cos 3 mpid 101</pre>	Begins configuring the receiver on the responder and enters IP SLA Y.1731 delay configuration mode. <ul style="list-style-type: none"> The <i>source-mp-id</i> or <i>source-address</i> configured by this command corresponds to that of the MEP being configured. <p>Note The session with mac-address will not be inactivated when there is CFM error.</p>
Step 5	aggregate interval <i>seconds</i> Example: <pre>Router(config-sla-y1731-delay)# aggregate interval 900</pre>	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 6	distribution {delay delay-variation} one-way <i>number-of-bins boundary[,...,boundary]</i> Example: <pre>Router(config-sla-y1731-delay)# distribution delay-variation one-way 5 5000,10000,15000,20000,-1</pre>	(Optional) Specifies measurement type and configures bins for statistics distributions kept.
Step 7	frame offset <i>offset-value</i> Example: <pre>Router(config-sla-y1731-delay)# frame offset 1</pre>	(Optional) Sets the value for calculating delay variation rates.
Step 8	history interval <i>intervals-stored</i> Example: <pre>Router(config-sla-y1731-delay)# history interval 2</pre>	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 9	max-delay <i>milliseconds</i> Example: <pre>Router(config-sla-y1731-delay)# max-delay 5000</pre>	(Optional) Sets the amount of time an MEP waits for a frame.
Step 10	owner <i>owner-id</i> Example: <pre>Router(config-sla-y1731-delay)# owner admin</pre>	(Optional) Configures the owner of an IP SLAs operation.

	Command or Action	Purpose
Step 11	end Example: <pre>Router(config-sla-y1731-delay)# end</pre>	Exits to privileged EXEC mode.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps, see the "Configuring Proactive Threshold Monitoring" module of the *IP SLAs Configuration Guide*.

When you are finished configuring proactive threshold monitoring for this MEP, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Configuring the Sender MEP on the Source Router

Before you begin

- Time synchronization is required between the source and destination devices in order to provide accurate one-way delay (latency) or delay-variation measurements. Configure either Precision Time Protocol (PTP) or Network Time Protocol (NTP) on both the source and destination devices.
- The receiver MEP must be configured, including proactive threshold monitoring, and scheduled before you configure the sender MEP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **ethernet y1731 delay 1DM domain domain-name {evc evc-id | vlan vlan-id} {mpid target-mp-id | mac-address target-address} cos cos {source {mpid source-mp-id | mac-address source-address}}**
5. **aggregate interval seconds**
6. **frame interval milliseconds**
7. **frame size bytes**
8. **history interval intervals-stored**
9. **owner owner-id**
10. **end**

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.

	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 500	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ethernet y1731 delay 1DM domain domain-name {evc evc-id vlan vlan-id} {mpid target-mp-id mac-address target-address} cos cos {source {mpid source-mp-id mac-address source-address}} Example: Router(config-ip-sla)# ethernet y1731 delay 1DM domain xxx evc yyy mpid 101 cos 3 source mpid 100	Begins configuring a dual-ended Ethernet delay operation and enters IP SLA Y.1731 delay configuration mode. Note The session with mac-address will not be inactivated when there is CFM error.
Step 5	aggregate interval seconds Example: Router(config-sla-y1731-delay)# aggregate interval 900	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 6	frame interval milliseconds Example: Router(config-sla-y1731-delay)# frame interval 100	(Optional) Sets the gap between successive frames.
Step 7	frame size bytes Example: Router(config-sla-y1731-delay)# frame size 64	(Optional) Sets the padding size for frames.
Step 8	history interval intervals-stored Example: Router(config-sla-y1731-delay)# history interval 2	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.

	Command or Action	Purpose
Step 9	owner <i>owner-id</i> Example: Router(config-sla-y1731-delay)# owner admin	(Optional) Configures the owner of an IP SLAs operation.
Step 10	end Example: Router(config-sla-y1731-delay)# end	Exits to privileged EXEC mode.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps, see the "Configuring Proactive Threshold Monitoring" module of the *IP SLAs Configuration Guide*.

When you are finished configuring proactive threshold monitoring for this MEP, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation

Perform this task to configure a sender MEP on the source device.

Before you begin

- Time synchronization is required between the source and destination devices in order to provide accurate one-way delay (latency) or delay-variation measurements. Configure either Precision Time Protocol (PTP) or Network Time Protocol (NTP) on both the source and destination devices.

**Note**

To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **ethernet y1731 delay {DMM | DMMv1} [burst] domain *domain-name* {evc *evc-id* | vlan *vlan-id*} {mpid *target-mp-id* | mac-address *target-address*} cos *cos* {source {mpid *source-mp-id* | mac-address *source-address*} }**
5. **clock sync**
6. **aggregate interval *seconds***
7. **distribution {delay | delay-variation} one-way *number-of-bins boundary[,...,boundary]***

Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation

8. **frame interval** *milliseconds*
9. **frame offset** *offset-value*
10. **frame size** *bytes*
11. **history interval** *intervals-stored*
12. **max-delay** *milliseconds*
13. **owner** *owner-id*
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config-term)# ip sla 10</pre>	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ethernet y1731 delay {DMM DMMv1} [burst] domain domain-name {evc evc-id vlan vlan-id} {mpid target-mp-id mac-address target-address} cos cos {source {mpid source-mp-id mac-address source-address}} Example: <pre>Device(config-ip-sla)# ethernet y1731 delay dmm domain xxx evc yyy mpid 101 cos 4 source mpid 100</pre>	Begins configuring a single-ended Ethernet delay operation and enters IP SLA Y.1731 delay configuration mode. <ul style="list-style-type: none"> • To configure concurrent operations, use the DMMv1 keyword with this command. Repeat the preceding two steps to each concurrent operation, to be added to a single IP SLA operation number. Concurrent operations are supported for a given EVC, CoS, and remote MEP combination, or for multiple MEPs for a given multipoint EVC. <p>Note The session with mac-address will not be inactivated when there is CFM error.</p>
Step 5	clock sync Example: <pre>Device(config-sla-y1731-delay)# clock sync</pre>	(Optional) Indicates that the end points are synchronized and thus allows the operation to calculate one-way delay measurements.

	Command or Action	Purpose
Step 6	aggregate interval <i>seconds</i> Example: Device(config-sla-y1731-delay)# aggregate interval 900	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 7	distribution {delay delay-variation} one-way <i>number-of-bins boundary[,...boundary]</i> Example: Device(config-sla-y1731-delay)# distribution delay-variation one-way 5 5000, 10000,15000,20000,-1	(Optional) Specifies measurement type and configures bins for statistics distributions kept.
Step 8	frame interval <i>milliseconds</i> Example: Device(config-sla-y1731-delay)# frame interval 100	(Optional) Sets the gap between successive frames.
Step 9	frame offset <i>offset-value</i> Example: Device(config-sla-y1731-delay)# frame offset 1	(Optional) Sets value for calculating delay variation values.
Step 10	frame size <i>bytes</i> Example: Device(config-sla-y1731-delay)# frame size 32	(Optional) Configures padding size for frames.
Step 11	history interval <i>intervals-stored</i> Example: Device(config-sla-y1731-delay)# history interval 2	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 12	max-delay <i>milliseconds</i> Example: Device(config-sla-y1731-delay)# max-delay 5000	(Optional) Sets the amount of time an MEP waits for a frame.
Step 13	owner <i>owner-id</i> Example:	(Optional) Configures the owner of an IP SLAs operation.

Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation

	Command or Action	Purpose
	Device(config-sla-y1731-delay)# owner admin	
Step 14	end Example: <pre>Device(config-sla-y1731-delay)# end</pre>	Exits to privileged EXEC mode.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps, see the "Configuring Proactive Threshold Monitoring" module of the *IP SLAs Configuration Guide*.

When you are finished configuring proactive threshold monitoring for this operation, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation



Note To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

Perform this task to configure a sender MEP on the source device.

Before you begin

- Class of Service (CoS)-level monitoring must be enabled on MEPs associated to the Ethernet frame loss operation by using the **monitor loss counter** command on the devices at both ends of the operation. See the *Cisco IOS Carrier Ethernet Command Reference* for command information. See the "Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations" section for configuration information.



Note Cisco IOS Y.1731 implementation allows monitoring of frame loss for frames on an EVC regardless of the CoS value (any CoS or Aggregate CoS cases). See the "Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations" section for configuration information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**

4. **ethernet y1731 loss {LMM | SLM} [burst] domain domain-name {evc evc-id | vlan vlan-id} {mpid target-mp-id | mac-address target-address} CoS CoS {source {mpid source-mp-id | mac-address source-address}}**
5. **aggregate interval seconds**
6. **availability algorithm {sliding-window | static-window}**
7. **frame consecutive value**
8. **frame interval milliseconds**
9. **history interval intervals-stored**
10. **owner owner-id**
11. **exit**
12. **exit**
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config-term)# ip sla 11</pre>	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ethernet y1731 loss {LMM SLM} [burst] domain domain-name {evc evc-id vlan vlan-id} {mpid target-mp-id mac-address target-address} CoS CoS {source {mpid source-mp-id mac-address source-address}} Example: <pre>Device(config-ip-sla)# ethernet y1731 loss LMM domain xxx vlan 12 mpid 34 CoS 4 source mpid 23</pre>	Begins configuring a single-ended Ethernet frame loss ratio operation and enters IP SLA Y.1731 loss configuration mode. <ul style="list-style-type: none"> To configure concurrent operations, use the SLM keyword with this command. Repeat the preceding two steps to configure each concurrent operation to be added to a single IP SLA operation number. Concurrent operations are supported for a given EVC, CoS, and remote-MEP combination, or for multiple MEPs for a given multipoint EVC. <p>Note The session with mac-address will not be inactivated when there is CFM error.</p>

Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation

	Command or Action	Purpose
Step 5	aggregate interval <i>seconds</i> Example: Device(config-sla-y1731-loss)# aggregate interval 900	(Optional) Configures the length of time during which performance measurements are conducted and the results stored.
Step 6	availability algorithm { sliding-window static-window } Example: Device(config-sla-y1731-loss)# availability algorithm static-window	(Optional) Specifies availability algorithm used.
Step 7	frame consecutive <i>value</i> Example: Device(config-sla-y1731-loss)# frame consecutive 10	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status.
Step 8	frame interval <i>milliseconds</i> Example: Device(config-sla-y1731-loss)# frame interval 100	(Optional) Sets the gap between successive frames.
Step 9	history interval <i>intervals-stored</i> Example: Device(config-sla-y1731-loss)# history interval 2	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 10	owner <i>owner-id</i> Example: Device(config-sla-y1731-delay)# owner admin	(Optional) Configures the owner of an IP SLAs operation.
Step 11	exit Example: Device(config-sla-y1731-delay)# exit	Exits to IP SLA configuration mode.
Step 12	exit Example:	Exits to global configuration mode.

	Command or Action	Purpose
	Device(config-ip-sla)# exit	
Step 13	exit Example: <pre>Device(config)# exit</pre>	Exits to privileged EXEC mode.

What to do next

When you are finished configuring this MEP, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month]} | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month]} | pending | now | after hh:mm [:ss]]]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: Device# show ip sla configuration	(Optional) Displays IP SLAs configuration details.

Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Example: Dual-Ended Ethernet Delay Operation

The following sample output shows the configuration, including default values, of a receiver MEP on the responder device for a dual-ended Ethernet delay or delay variation operation:

```
Device# show ip sla configuration 501

IP SLAs Infrastructure Engine-III
Entry number: 501
Owner: admin
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: xxx
ReceiveOnly: TRUE
Evc: yyy
Local Mpid: 101
CoS: 3
    Max Delay: 5000
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
    Aggregation Period: 900
    Frame offset: 1
    Distribution Delay One-Way:
        Number of Bins 10
        Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
    Distribution Delay-Variation One-Way:
        Number of Bins 10
        Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
    Number of intervals: 2
```

The following sample output shows the configuration, including default values, of the sender MEP for a dual-ended IP SLAs Ethernet delay or delay variation operation:

```
Device# show ip sla configuration 500

IP SLAs Infrastructure Engine-III
Entry number: 500
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: yyy
ReceiveOnly: FALSE
Evc: xxx
Target Mpid: 101
Source Mpid: 100
```

Example: Frame Delay and Frame Delay Variation Measurement Configuration

```

CoS: 3
    Request size (Padding portion): 64
    Frame Interval: 1000
    Threshold (milliseconds): 5000
    .
    .
    Statistics Parameters
        Aggregation Period: 900
        Frame offset: 1
    History
        Number of intervals: 22

```

Example: Frame Delay and Frame Delay Variation Measurement Configuration

The following sample output shows the performance monitoring session summary:

```
Device# show ethernet cfm pm session summary
```

```

Number of Configured Session : 2
Number of Active Session: 2
Number of Inactive Session: 0

```

The following sample output shows the active performance monitoring session:

```
Device# show ethernet cfm pm session active
```

Display of Active Session

EPM-ID	SLA-ID	Lvl/Type/ID/Cos/Dir	Src-Mac-address	Dst-Mac-address
0	10	3/BD-V/10/2/Down	d0c2.8216.c9d7	d0c2.8216.27a3
1	11	3/BD-V/10/3/Down	d0c2.8216.c9d7	d0c2.8216.27a3

```
Total number of Active Session: 2
```

```
Device# show ethernet cfm pm session db 0
```

TX Time FWD Sec:nSec	RX Time FWD Sec:nSec	Frame Delay Sec:nSec
234:526163572	245:305791416	
245:306761904	234:527134653	0:593
235:528900628	246:308528744	
246:309452848	235:529825333	0:601
236:528882716	247:308511128	
247:309450224	236:529822413	0:601
237:526578788	248:306207432	
248:307157936	237:527529885	0:593
238:527052156	249:306681064	
249:307588016	238:527959717	0:609
239:526625044	250:306254200	
250:307091888	239:527463325	0:593

240:528243204	251:307872648	0:585
251:308856880	240:529228021	

Example: Sender MEP for a Single-Ended Ethernet Delay Operation

The following sample output shows the configuration, including default values, of the sender MEP for a single-ended IP SLAs Ethernet delay operation:

```
Router# show ip sla configuration 10

IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: xxx
Vlan: yyy
Target Mpid: 101
Source Mpid: 100
CoS: 4
    Max Delay: 5000
    Request size (Padding portion): 64
    Frame Interval: 1000
    Clock: Not In Sync
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
    Aggregation Period: 900
    Frame offset: 1
    Distribution Delay Two-Way:
        Number of Bins 10
        Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
    Distribution Delay-Variation Two-Way:
        Number of Bins 10
        Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
    Number of intervals: 2
```

Example: Sender MEP for a Single-Ended Ethernet Frame Loss Operation

The following output shows the configuration, including default values, of the sender MEP in a basic single-ended IP SLAs Ethernet frame loss ratio operation with a start-time of now:

```
Router# show ip sla configuration 11

IP SLAs Infrastructure Engine-III
Entry number: 11
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Loss Operation
Frame Type: LMM
Domain: xxx
```

Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

```

Vlan: 12
Target Mpid: 34
Source Mpid: 23
CoS: 4
    Request size (Padding portion): 0
    Frame Interval: 1000
Schedule:
    Operation frequency (seconds): 60 (not considered if randomly scheduled)
    Next Scheduled Start Time: Start Time already passed
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): ActiveThreshold (milliseconds): 5000
Statistics Parameters
    Aggregation Period: 900
    Frame consecutive: 10
    Availability algorithm: static-window
History
    Number of intervals: 2

```

Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Carrier Ethernet commands	Cisco IOS Carrier Ethernet Command Reference
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference
Ethernet CFM	“Configuring Ethernet Connectivity Fault Management in a Service Provider Network” module of the <i>Cisco IOS Carrier Ethernet Configuration Guide</i>
Network Time Protocol (NTP)	“Configuring NTP” module of the <i>Cisco IOS Network Management 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 and RFCs

Standard/RFC	Title
ITU-T Y.1731	<i>OAM functions and mechanisms for Ethernet-based networks</i>
No specific RFCs are supported by the features in this document.	--

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) 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 17: Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)

Feature Name	Releases	Feature Information
IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)	15.1(2)S 15.4(1)S	<p>This feature provides the capability to gather Ethernet-layer network performance metrics, such as frame delay, frame delay variation, and frame loss ratio (as defined by the ITU-T Y.1737 networking standard), for assisting with IP SLAs assurance and capacity planning.</p> <p>The following commands were introduced or modified: aggregate interval, availability, distribution, etherent y1731 delay, etherent y1731 delay receive, etherent y1731 loss, frame consecutive, frame interval, frame offset, frame size, history interval, ip sla reaction-configuration, max-delay, owner, show ip sla history interval.</p> <p>In Cisco IOS Release 15.4(1)S, support was added for Cisco ASR 900 Series.</p>
IP SLA Support for ETH-SLM (Ethernet Synthetic Loss Measurement in Y1731)	15.3(2)S 15.4(1)S	<p>Y.1731 Performance Monitoring (PM) provides a standard Ethernet PM function that includes measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group.</p> <p>In Cisco IOS Release 15.3(2)S, support was added for Cisco ASR 900 Series.</p> <p>In Cisco IOS Release 15.4(1)S, support was added for Cisco ASR 900 Series.</p>
Y1731 MIB Support through existing IPSLA MIBs	15.2(2)S	Support was added for reporting threshold events and collecting performance statistics for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operations using SNMP.

Feature Name	Releases	Feature Information
Y.1731 Performance Monitoring	15.2(1)S	Support was added for Cisco ME 3600X Series and 3800X Series Ethernet Access Switches.



CHAPTER 9

IPSLA Y1731 On-Demand and Concurrent Operations

This module describes how to configure the IPSLA Y1731 SLM Feature Enhancements feature for enabling real-time Ethernet service troubleshooting for users without configuration privileges. This feature supports on-demand Synthetic Loss Measurement (SLM) operations that can be run by issuing a single command in privileged EXEC mode.

- [Finding Feature Information, on page 139](#)
- [Prerequisites for ITU-T Y.1731 Operations, on page 139](#)
- [Restrictions for IP SLAs Y.1731 On-Demand Operations, on page 140](#)
- [Information About IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 140](#)
- [How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 141](#)
- [Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 143](#)
- [Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 146](#)
- [Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 147](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for ITU-T Y.1731 Operations

IEEE-compliant Connectivity Fault Management (CFM) must be configured and enabled for Y.1731 performance monitoring to function.



Note Y1731 is supported on Port Channel interfaces.

Restrictions for IP SLAs Y.1731 On-Demand Operations

- SNMP is not supported for reporting threshold events or collecting performance statistics for on-demand operations.
- On-demand operation statistics are not stored and are not supported by the statistic history and aggregation functions.

Information About IP SLAs Y.1731 On-Demand and Concurrent Operations

IPSLA Y1731 SLM Feature Enhancements

On-demand IP SLAs Synthetic Loss Measurement (SLM) operations, in the IPSLA Y1731 SLM Feature Enhancements feature, enable users without configuration access to perform real-time troubleshooting of Ethernet services. There are two operational modes for on-demand operations: direct mode that creates and runs an operation immediately and referenced mode that starts and runs a previously configured operation.

- In the direct mode, a single command can be used to create multiple pseudo operations for a range of class of service (CoS) values to be run, in the background, immediately. A single command in privileged EXEC mode can be used to specify frame size, interval, frequency, and duration for the direct on-demand operation. Direct on-demand operations start and run immediately after the command is issued.
- In the referenced mode, you can start one or more already-configured operations for different destinations, or for the same destination, with different CoS values. Issuing the privileged EXEC command creates a pseudo version of a proactive operation that starts and runs in the background, even while the proactive operation is running.
- Once an on-demand operation is completed, statistical output is displayed on the console. On-demand operation statistics are not stored and are not supported by the statistic history and aggregation functions.
- After an on-demand operation is completed, and the statistics handled, the direct and referenced on-demand operation is deleted. The proactive operations are not deleted and continue to be available to be run in referenced mode, again.

A concurrent operation consists of a group of operations, all configured with the same operation ID number, that run concurrently. Concurrent operations are supported for a given Ethernet Virtual Circuit (EVC), CoS, and remote Maintenance End Point (MEP) combination, or for multiple MEPs for a given multipoint EVC, for delay or loss measurements. A new keyword was added to the appropriate commands to specify that concurrent Ethernet frame Delay Measurement (ETH-DM) synthetic frames are sent during the operation.

The IPSLA Y.1731 SLM Feature Enhancements feature also supports burst mode for concurrent operations, one-way dual-ended, and single-ended delay and delay variation operations, as well as for single-ended loss operations. A new keyword was added to the appropriate commands to support bursts of PDU transmission during an aggregation interval. The maximum number of services monitored is 50 every 30 minutes, with an average of 25 services every 2 hours.

How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations

Configuring a Direct On-Demand Operation on a Sender MEP

Before you begin

Class of Service (CoS)-level monitoring must be enabled on MEPs associated to the Ethernet frame loss operation by using the **monitor loss counter** command on the devices at both ends of the operation. See the *Cisco IOS Carrier Ethernet Command Reference* for command information. See the “Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations” section for configuration information.



Note The Cisco IOS Y.1731 implementation allows monitoring of frame loss on an EVC regardless of the CoS value (any CoS or aggregate CoS cases). See the “Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations” section for configuration information.

SUMMARY STEPS

1. **enable**
2. **ip sla on-demand ethernet {DMMv1 | SLM} domain domain-name {evc evc-id | vlan vlan-id} {mpid target-mp-id | mac-address target-address} cos cos {source {mpid source-mp-id | mac-address source-address}} {continuous [interval milliseconds] | burst [interval milliseconds] [number number-of-frames] [frequency seconds]} [size bytes] aggregation seconds {duration seconds | max number-of-packets}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	ip sla on-demand ethernet {DMMv1 SLM} domain domain-name {evc evc-id vlan vlan-id} {mpid target-mp-id mac-address target-address} cos cos {source {mpid source-mp-id mac-address source-address}} {continuous [interval milliseconds] burst [interval milliseconds] [number number-of-frames] [frequency seconds]} [size bytes] aggregation seconds {duration seconds max number-of-packets} Example:	Creates and runs an on-demand operation in direct mode. <ul style="list-style-type: none"> • To create and run concurrent on-demand operations, configure this command using the DMMv1 keyword. • Statistical output is posted on the console after the operation is finished. • Repeat this step for each on-demand operation to be run. • After an on-demand operation is finished and the statistics handled, the operation is deleted.

Configuring a Referenced On-Demand Operation on a Sender MEP

Command or Action	Purpose
Device# ip sla on-demand ethernet SLM domain xxx vlan 12 mpid 34 cos 4 source mpid 23 continuous aggregation 10 duration 60	

Configuring a Referenced On-Demand Operation on a Sender MEP



Note After an on-demand operation is finished and the statistics handled, the on-demand version of the operation is deleted.

Before you begin

- Single-ended and concurrent Ethernet delay, or delay variation, and frame loss operations to be referenced must be configured. See the “Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations” module of the *IP SLAs Configuration Guide*.

SUMMARY STEPS

- enable
- ip sla on-demand ethernet [dmmv1 | slm] *operation-number {duration seconds | max number-of-packets}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	ip sla on-demand ethernet [dmmv1 slm] <i>operation-number {duration seconds max number-of-packets}</i> Example: Device# ip sla on-demand ethernet slm 11 duration 38	Creates and runs a pseudo operation of the operation being referenced, in the background. • Statistical output is posted on the console after the operation is finished. • Repeat this step for each on-demand operation to be run.

Configuring an IP SLAs Y.1731 Concurrent Operation on a Sender MEP

To configure concurrent Ethernet delay, delay variation, and frame loss operations, see the “Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations” module of the

IP SLAs Configuration Guide.

Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations

Example: On-Demand Operation in Direct Mode

```
Device# ip sla on-demand ethernet SLM domain xxx vlan 10 mpid 3 cos 1 source mpid 1 continuous
aggregation 35 duration 38

Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:

Interval 1
Start time: *20:17:41.535 PST Wed May 16 2012
End time: *20:18:16.535 PST Wed May 16 2012
Number of measurements initiated: 35
Number of measurements completed: 35
Flag: OK

Forward
Number of Observations 3
Available indicators: 0
Unavailable indicators: 3
Tx frame count: 30
Rx frame count: 30
Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
Cumulative - (FLR % ): 000.00%
Timestamps forward:
Min - *20:18:10.586 PST Wed May 16 2012
Max - *20:18:10.586 PST Wed May 16 2012
Backward
Number of Observations 3
Available indicators: 0
Unavailable indicators: 3
Tx frame count: 30
Rx frame count: 30
Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
Cumulative - (FLR % ): 000.00%
Timestamps backward:
Min - *20:18:10.586 PST Wed May 16 2012
Max - *20:18:10.586 PST Wed May 16 2012
Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:

Interval 1
Start time: *20:17:41.535 PST Wed May 16 2012
End time: *20:18:16.535 PST Wed May 16 2012
Number of measurements initiated: 35
Number of measurements completed: 35
Flag: OK
```

Example: On-Demand Operation in Referenced Mode

```

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012

```

Example: On-Demand Operation in Referenced Mode

```

Device(config)# ip sla 11
Device(config-ip-sla)# ethernet y1731 loss SLM domain xxx vlan 10 mpid 3 cos 1 source mpid
  1
Device(config-sla-y1731-loss)# end
Device# ip sla on-demand ethernet slm 11 duration 38

Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:

Interval 1
Start time: *20:17:41.535 PST Wed May 16 2012
End time: *20:18:16.535 PST Wed May 16 2012
Number of measurements initiated: 35
Number of measurements completed: 35
Flag: OK

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0

```

```

Unavailable indicators: 3
Tx frame count: 30
Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
    Cumulative - (FLR % ): 000.00%
Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:

Interval 1
Start time: *20:17:41.535 PST Wed May 16 2012
End time: *20:18:16.535 PST Wed May 16 2012
Number of measurements initiated: 35
Number of measurements completed: 35
Flag: OK

Forward
Number of Observations 3
Available indicators: 0
Unavailable indicators: 3
Tx frame count: 30
Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
    Cumulative - (FLR % ): 000.00%
Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
Number of Observations 3
Available indicators: 0
Unavailable indicators: 3
Tx frame count: 30
Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
    Cumulative - (FLR % ): 000.00%
Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012

```

IP SLA Reconfiguration Scenarios

IP SLA Reconfiguration Scenarios

IP SLA must be reconfigured in the following scenarios:

- When an Ethernet service instance is disabled on the interface using the **service instance ethernet** command.
- When the local MEP is removed using the **no cfm mep domain *domain-name* mpid *mpid*** command.

- When the configuration of an interface is reset to its default values, using the **default interface** command.
- When an interface configuration is removed using the **no interface** command.
- When the Ethernet Connectivity Fault Management (CFM) distribution is disabled using the **no ethernet cfm global** and **no ethernet cfm ieee** commands.

Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Carrier Ethernet commands	Cisco IOS Carrier Ethernet Command Reference
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference
Ethernet CFM for ITU-T Y.1731	“ITU-T Y.1731 Performance Monitoring in a Service Provider Network” module of the <i>Carrier Ethernet Configuration Guide</i>
Ethernet operations	“Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations” module of the <i>IP SLAs Configuration Guide</i>
Network Time Protocol (NTP)	“Configuring NTP” module of the <i>Network Management Configuration Guide</i>

Standards and RFCs

Standard/RFC	Title
ITU-T Y.1731	<i>OAM functions and mechanisms for Ethernet-based networks</i>

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 18: Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations

Feature Name	Releases	Feature Information
IPSLA Y1731 SLM Feature Enhancements	15.3(1)S	This feature enhancement allows you to run on-demand Synthetic Loss Measurement (SLM) operations, independent from previously scheduled operations, for the purpose of troubleshooting Etherent services in your network. The following commands were introduced or modified: ethernet y1731 delay , ethernet y1731 loss , ip sla on-demand ethernet .

Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations

Feature Name	Releases	Feature Information
Y.1731 Performance Monitoring	15.2(1)S	Support was added for Cisco ME 3600X Series and 3800X Series Ethernet Access Switches.



CHAPTER 10

Configuring IP SLA - Service Performance Testing

This module describes how to configure the ITU-T Y.1564 Ethernet service performance test methodology to measure the ability of a network device to carry traffic at the configured data rate.

- [Finding Feature Information, on page 149](#)
- [Prerequisites for IP SLA - Service Performance Testing, on page 149](#)
- [Restrictions for IP SLA - Service Performance Operation, on page 149](#)
- [Information About IP SLA - Service Performance Testing, on page 150](#)
- [How to Configure IP SLA - Service Performance Testing, on page 151](#)
- [Configuration Examples for IP SLA - Service Performance Testing, on page 157](#)
- [Additional References for IP SLA - Service Performance Testing, on page 159](#)
- [Feature Information for IP SLA - Service performance Testing, on page 159](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP SLA - Service Performance Testing

Ensure that the direction configured for the **measurement-type direction {internal | external}** and the **profile traffic direction {internal | external}** commands is the same.

Restrictions for IP SLA - Service Performance Operation

- Traffic generation mode is not supported in Cisco IOS Release 15.3(2)S.
- One-way statistics collection is not supported in Cisco IOS Release 15.3(2)S.

Information About IP SLA - Service Performance Testing

ITU Y.1564

Y.1564 is an Ethernet service activation and performance test methodology for turning up, installing and troubleshooting Ethernet-based services. This test methodology allows for complete validation of Ethernet service level agreements (SLAs) in a single test.

The three key objectives for Y.1564 are as follows:

- To serve as a network SLAs validation tool, ensuring that a service meets its guaranteed performance settings in a controlled test time.
- To ensure that all services carried by the network meet their SLAs objectives at the maximum committed rate, proving that network devices and paths can support all the traffic as designed under maximum load.
- To perform medium- and long-term service testing, confirming that a network element can properly carry all services while under stress during a soaking period.

The following Key Performance Indicators (KPI) metrics are collected to ensure that the configured SLAs is met for the service/stream. These are service acceptance criteria metrics.

- Information Rate (IR) or throughput—Measures the maximum rate at which none of the offered frames are dropped by the device under test (DUT). This measurement translates into the available bandwidth of the Ethernet virtual connection (EVC).
- Frame Transfer Delay (FTD) or latency—Measures the round-trip time (RTT) taken by a test frame to travel through a network device or across the network and back to the test port .
- Frame Loss Ratio (FLR)—Measures the number of packets lost over the total number of packets sent. Frame loss can be due to a number of issues such as network congestion or errors during transmissions.
- Frame Delay Variation (FDV) or jitter—Measures the variations in the time delay between packet deliveries.

Service Performance Operations

Forwarding devices (switches and routers) and network interface units are the basis of any network as they interconnect segments. If a service is not correctly configured on any one of these devices within the end-to-end path, network performance can be greatly affected, leading to potential service outages and network-wide issues such as congestion and link failures. Service performance testing is designed to measure the ability of device under test (DUT) or network under test to properly forward in different states. The Cisco implementation of ITU-T Y.1564 includes the following service performance tests:

- Minimum data rate to CIR—Bandwidth is generated from the minimum data rate to the committed information rate (CIR) for the test stream. KPI for Y.1564 are then measured to ensure that the configured service acceptance criteria (SAC) are met.
- CIR to EIR—Bandwidth is ramped up from the CIR to the excess information rate (EIR) for the test stream. Because EIR is not guaranteed, only the transfer rate is measured to ensure that CIR is the minimum bandwidth up to the maximum EIR. Other KPI are not measured.

Service performance supports four operational modes: two-way statistics collection, one-way statistics collection, passive measurement mode, and traffic generator mode. Statistics are calculated, collected, and reported to the IP SLAs module. The statistics database keeps historical statistics for the operations that have been executed.

For two-way statistics collection, all measurements are collected by the sender. In order for two-way statistics to work, the remote target must be in loopback mode. Loopback mode enables traffic sent from the sender to go to the target and be returned to the sender.

One-way statistics are collected by the responder. Control messages are sent from the sender to a responder to enable and retrieve the remote statistics.

Passive measurement mode is enabled by excluding a configured traffic profile. A passive measurement operation does not generate live traffic. The operation only collects statistics for the target configured for the operation.

The traffic generator mode sends traffic only. No statistics are collected.

How to Configure IP SLA - Service Performance Testing

Configuring a Service Performance Operation

Perform the following steps to define the parameters for a single service performance test stream.

Before you begin

- The service instance for the Ethernet Flow Point (EFP) must be configured. For configuration information, see your hardware configuration guide.
- For two-way statistics calculations, the destination interface must be in loopback mode. For information, see the *Interface and Hardware Component Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **service-performance type type dest-mac-addr mac-address interface interface service instance id**
5. **aggregation interval buckets buckets**
6. **description description**
7. **duration time seconds**
8. **frequency {interation interation-number delay seconds}**
9. **frequency time seconds}**
10. **measurement-type direction {external | internal}**
11. **signature sequence**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Configures an IP SLAs operation and enters IP SLA configuration mode.
Step 4	service-performance type <i>type</i> dest-mac-addr <i>mac-address</i> interface <i>interface</i> service instance <i>id</i> Example: Device(config-ip-sla)# service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitethernet0/4 service instance 100	Configures a service performance operation and enters service performance configuration mode.
Step 5	aggregation interval buckets <i>buckets</i> Example: Device(config-ip-sla-service-performance)# aggregation interval buckets 5	(Optional) Configures number of interval buckets to be kept.
Step 6	description <i>description</i> Example: Device(config-ip-sla-service-performance)# description With all operations	(Optional)
Step 7	duration time <i>seconds</i> Example: Device(config-ip-sla-service-performance)# duration time 20	(Optional)
Step 8	frequency {interation <i>interation-number</i> delay <i>seconds</i>} Example: Device(config-ip-sla-service-performance)# frequency interation 1 delay 5	(Optional) Specifies how often and for how long the operation runs.
Step 9	frequency time <i>seconds</i>} Example: Device(config-ip-sla-service-performance)# frequency time 30	(Optional) Specifies how often and for how long the operation runs.

	Command or Action	Purpose
Step 10	measurement-type direction {external internal} Example: Device(config-ip-sla-service-performance)# measurement-type direction external	(Optional) Configures measurement metrics type.
Step 11	signature sequence Example: Device(config-ip-sla-service-performance)# signature 05060708	(Optional) Configures payload contents.
Step 12	end Example: Device(config-ip-sla-service-performance)# end	returns to privileged EXEC mode.

Configuring Service Performance Profiles on the Sender

Perform these steps to configure profiles for generating live traffic.



Note

Do not configure a traffic profile if you are configuring an operation for passive measurement mode.

Before you begin

The service performance operation to which the profile is to be applied must be configured. For configuration information, see the “Configuring a Service Performance Operation” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **profile traffic direction {external | internal}**
5. **rate-step *kbps* [*kbps* ... *kbps*]**
6. **exit**
7. **profile packet**
8. **inner-cos *cos-number***
9. **outer-cos *cos-number***
10. **inner-vlan *vlan-id***
11. **outer-vlan *vlan-id***
12. **packet-size *size***
13. **src-mac-addr *mac-address***
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Configures an IP SLA operation.
Step 4	profile traffic direction {external internal} Example: Device(config-ip-sla-service-performance)# profile traffic direction internal	Configures a traffic profile for generating live traffic.
Step 5	rate-step kbps [kbps ... kbps] Example: Device(config-ip-sla-service-performance-traffic)#rate-step 1000 2000	Configures a list of rate steps for live traffic.
Step 6	exit Example: Device(config-ip-sla-service-performance-traffic)# exit	
Step 7	profile packet Example: Device(config-ip-sla-service-performance)# profile packet	Configures a packet profile for live traffic.
Step 8	inner-cos cos-number Example: Device(config-ip-sla-service-performance-packet)# inner-cos 6	Sets inner-loop CoS in the packet profile.
Step 9	outer-cos cos-number Example: Device(config-ip-sla-service-performance-packet)# outer-cos 6	Sets outer-loop CoS in the packet profile.
Step 10	inner-vlan vlan-id Example:	Specifies the inner-loop VLAN in the packet profile.

	Command or Action	Purpose
	Device(config-ip-sla-service-performance-packet)# inner-vlan 100	
Step 11	outer-vlan <i>vlan-id</i> Example: Device(config-ip-sla-service-performance-packet)# outer-vlan 100	Specifies the outer-loop VLAN in the packet profile.
Step 12	packet-size <i>size</i> Example: Device(config-ip-sla-service-performance-packet)# packet-size 512	(Optional) Specifies packet size in the packet profile.
Step 13	src-mac-addr <i>mac-address</i> Example: Device(config-ip-sla-service-performance-packet)# src-mac-addr 4055.398d.8d4c	Specifies source device in packet profile.
Step 14	end Example: Device(config-ip-sla-service-performance)# end	Returns to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule *operation-number* [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule *group-operation-number* *operation-id-numbers* {schedule-period *schedule-period-range* | schedule-together} [ageout seconds] frequency *group-operation-frequency* [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}}] [ageout seconds] [recurring] ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> Configures the scheduling parameters for an individual IP SLAs operation. Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays IP SLAs group schedule details.

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

Configuration Examples for IP SLA - Service Performance Testing

Example: Service Performance Operation

```

Device# show ip sla configuration 1
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
VLAN:
Interface: GigabitEthernet0/4
Service Instance: 10
EVC Name:
Duration Time: 20
Interval Buckets: 5

Signature:
05060708

Description: this is with all operation modes

Measurement Type:
throughput, loss
Direction: internal

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
Schedule:
    Operation frequency (seconds): 64 (not considered if randomly scheduled)
    Next Scheduled Start Time: Start Time already passed

```

Example: Passive Measurement Mode

```

Group Scheduled : FALSE
Randomly Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active

```

Example: Passive Measurement Mode

The following sample output displays the default configuration for a passive-measurement service performance operation. No live traffic will be generated for this operation because the traffic profile is not configured.

```

sla-asr901-1# show ip sla configuration 10

IP SLAs Infrastructure Engine-III
Entry number: 10
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
VLAN:
Interface: GigabitEthernet0/0
Service Instance: 10
EVC Name:
Duration Time: 30
Interval Buckets: 1

Signature:

Description:

Measurement Type:
  none
Direction: internal

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 0
Burst Duration: 0
Inter Burst Interval: 0
Rate Step (kbps):

Profile Packet:
Inner COS: Not Set
Outer COS: Not Set
Inner VLAN: Not Set
Outer VLAN: Not Set
Source MAC Address: 0000.0000.0000
EtherType: default
Packet Size: 64

```

Additional References for IP SLA - Service Performance Testing

Related Documents

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

Standards and RFCs

Standard/RFC	Title
ITU-T Y.1564	<i>Ethernet service activation test methodology</i>
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 SLA - Service performance Testing

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 SLA - Service performance Testing

Feature Name	Releases	Feature Information
IP SLA - Service Performance Testing	15.3(2)S 15.4(1)S	<p>The IP SLA - Service Performance Testing feature utilizes the ITU-T Y.1564 Ethernet service activation/performance test methodology for turning up, installing and troubleshooting Ethernet-based services. This test methodology allows for complete validation of Ethernet IP Service Level Agreements (SLAs) in a single test.</p> <p>The following commands were introduced or modified: aggregation interval, description (IP SLA), duration time, frequency (IP SLA service performance), inner-cos, inner-vlan, measurement-type, outer-cos, outer-vlan, packet size, profile packet, profile traffic, service-performance, show ip sla configuration, show ip sla group schedule signature (IP SLA).</p> <p>In Cisco IOS Release 15.4(1)S, support was added for the Cisco ASR 901S Router.</p>



CHAPTER 11

Configuring IP SLAs UDP Echo Operations

This module describes how to configure an IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) Echo operation to monitor end-to-end response time between a Cisco device and devices using IPv4 or IPv6. UDP echo accuracy is enhanced by using the Cisco IP SLAs Responder at the destination Cisco device. This module also demonstrates how the results of the UDP echo operation can be displayed and analyzed to determine how a UDP application is performing.

- [Finding Feature Information, on page 161](#)
- [Restrictions for IP SLAs UDP Echo Operations, on page 161](#)
- [Information About IP SLAs UDP Echo Operations, on page 162](#)
- [How to Configure IP SLAs UDP Echo Operations, on page 163](#)
- [Configuration Examples for IP SLAs UDP Echo Operations, on page 171](#)
- [Additional References, on page 171](#)
- [Feature Information for the IP SLAs UDP Echo Operation, on page 172](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs UDP Echo Operations

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

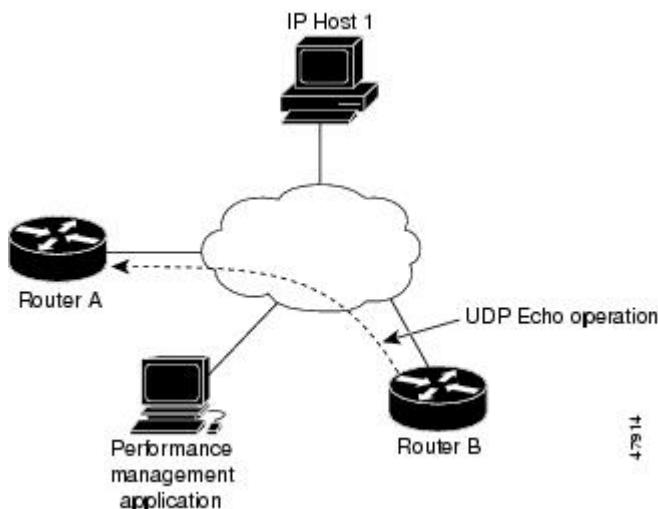
Information About IP SLAs UDP Echo Operations

UDP Echo Operation

The UDP echo operation measures end-to-end response time between a Cisco device and devices using IP. UDP is a transport layer (Layer 4) Internet protocol that is used for many IP services. UDP echo is used to measure response times and test end-to-end connectivity.

In the figure below Device A has been configured as an IP SLAs Responder and Device B is configured as the source IP SLAs device.

Figure 9: UDP Echo Operation



Response time (round-trip time) is computed by measuring the time taken between sending a UDP echo request message from Device B to the destination device--Device A--and receiving a UDP echo reply from Device A. UDP echo accuracy is enhanced by using the IP SLAs Responder at Device A, the destination Cisco device. If the destination device is a Cisco device, then IP SLAs sends a UDP datagram to any port number that you specified. Using the IP SLAs Responder is optional for a UDP echo operation when using Cisco devices. The IP SLAs Responder cannot be configured on non-Cisco devices.

The results of a UDP echo operation can be useful in troubleshooting issues with business-critical applications by determining the round-trip delay times and testing connectivity to both Cisco and non-Cisco devices.

How to Configure IP SLAs UDP Echo Operations

Configuring the IP SLAs Responder on a Destination Device

**Note**

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress *ip-address* port *port* vrf *vrf***
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla responder • ip sla responder udp-echo ipaddress <i>ip-address</i> port <i>port</i> vrf <i>vrf</i> Example: Device(config)# ip sla responder Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1	(Optional) Temporarily enables IP SLAs responder functionality on a Cisco device in response to control messages from the source. (Optional; required only if protocol control is disabled on the source.) Enables IP SLAs responder functionality on the specified IP address, port and VRF. • Protocol control is enabled by default.

Configuring a UDP Echo Operation on the Source Device

	Command or Action	Purpose
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a UDP Echo Operation on the Source Device

Perform only one of the following tasks:

Configuring a Basic UDP Echo Operation on the Source Device

Before you begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **udp-echo {destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname} source-port port-number] [control {enable | disable}]**
5. **data-pattern hex value**
6. **frequency seconds**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config)# ip sla 10</pre>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	udp-echo {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}] Example: Device(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. • Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target devices.
Step 5	data-pattern hex value Example: Device(config-ip-sla-udp)# data-pattern FFFFFFFF	(Optional) Sets a hexadecimal value for data pattern. The range is 0 to FFFFFFFF.
Step 6	frequency seconds Example: Device(config-ip-sla-udp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 7	end Example: Device(config-ip-sla-udp)# end	Returns to privileged EXEC mode.

What to do next

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

Configuring a UDP Echo Operation with Optional Parameters on the Source Device

Before you begin

If you are using an IP SLAs Responder in this operation, the responder must be configured on the destination device. See the "Configuring the IP SLAs Responder on the Destination Device."

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **udp-echo {destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname} source-port port-number] [control {enable | disable}]**
5. **history buckets-kept size**
6. **data-pattern hex-pattern**
7. **history distributions-of-statistics-kept size**
8. **history enhanced [interval seconds] [buckets number-of-buckets]**
9. **history filter {none | all | overThreshold | failures}**
10. **frequency seconds**

Configuring a UDP Echo Operation with Optional Parameters on the Source Device

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 Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	udp-echo {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}] Example: Device(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. • Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target devices.
Step 5	history buckets-kept size Example: Device(config-ip-sla-udp)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.

	Command or Action	Purpose
Step 6	data-pattern <i>hex-pattern</i> Example: Device(config-ip-sla-udp) # data-pattern	(Optional) Specifies the data pattern in an IP SLAs operation to test for data corruption.
Step 7	history distributions-of-statistics-kept <i>size</i> Example: Device(config-ip-sla-udp) # history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 8	history enhanced [<i>interval seconds</i>] [<i>buckets number-of-buckets</i>] Example: Device(config-ip-sla-udp) # history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 9	history filter {none all overThreshold failures} Example: Device(config-ip-sla-udp) # history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	frequency <i>seconds</i> Example: Device(config-ip-sla-udp) # frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	history hours-of-statistics-kept <i>hours</i> Example: Device(config-ip-sla-udp) # history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 12	history lives-kept <i>lives</i> Example: Device(config-ip-sla-udp) # history lives-kept 2	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	owner <i>owner-id</i> Example: Device(config-ip-sla-udp) # owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	request-data-size <i>bytes</i> Example: Device(config-ip-sla-udp) # request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.

Configuring a UDP Echo Operation with Optional Parameters on the Source Device

	Command or Action	Purpose
Step 15	history statistics-distribution-interval milliseconds Example: Device(config-ip-sla-udp)# history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	tag text Example: Device(config-ip-sla-udp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	threshold milliseconds Example: Device(config-ip-sla-udp)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	timeout milliseconds Example: Device(config-ip-sla-udp)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	Do one of the following: <ul style="list-style-type: none">• tos number• traffic-class number Example: Device(config-ip-sla-jitter)# tos 160 Example: Device(config-ip-sla-jitter)# traffic-class 160	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.
Step 20	flow-label number Example: Device(config-ip-sla-udp)# flow-label 112233	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 21	verify-data Example: Device(config-ip-sla-udp)# verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	exit Example: Device(config-ip-sla-udp)# exit	Exits UDP configuration submode and returns to global configuration mode.

What to do next

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

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • 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] 	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • ip sla group schedule <i>group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month]} pending now after hh:mm [:ss]}]</i> <p>Example:</p> <pre>Device(config)# ip sla schedule 10 life forever start-time now</pre> <pre>Device(config)# ip sla group schedule 10 schedule-period frequency</pre> <pre>Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now</pre> <pre>Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: Device# show ip sla configuration	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs UDP Echo Operations

Example Configuring a UDP Echo Operation

The following example configures an IP SLAs operation type of UDP echo that will start immediately and run indefinitely.

```
ip sla 5
  udp-echo 172.29.139.134 5000
  frequency 30
  request-data-size 160
  tos 128
  timeout 1000
  tag FLL-RO
ip sla schedule 5 life forever start-time now
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 862	Echo Protocol

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the IP SLAs UDP Echo Operation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 20: Feature Information for the IP SLAs UDP Echo Operation

Feature Name	Releases	Feature Information
IP SLAs - UDP Echo Operation	Cisco IOS 12.2(31)SB2 Cisco IOS 12.2(33)SRB1 Cisco IOS 12.2(33)SXH Cisco IOS 12.3(14)T Cisco IOS XE Release 2.1 Cisco IOS 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs User Datagram Protocol (UDP) jitter operation allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	Cisco IOS 12.2(33)SRC Cisco IOS 12.2(33)SB Cisco IOS 12.4(20)T Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG Cisco IOS 12.2(50)SY	Support was added for operability in IPv6 networks.



CHAPTER 12

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, on page 173](#)
- [Restrictions for IP SLAs HTTP Operations, on page 173](#)
- [Information About IP SLAs HTTP Operations, on page 174](#)
- [How to Configure IP SLAs HTTP Operations, on page 174](#)
- [Configuration Examples for IP SLAs HTTP Operations, on page 181](#)
- [Additional References, on page 182](#)
- [Feature Information for IP SLAs HTTP Operations, on page 183](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs HTTP Operations

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

Information About IP SLAs HTTP Operations

HTTP Operation

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

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

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

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

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

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

**Note**

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

How to Configure IP SLAs HTTP Operations

Configuring an HTTP GET Operation on the Source Device

**Note**

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

Perform only one of the following tasks:

Configuring a Basic HTTP GET Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **http {get | raw} *url* [**name-server ip-address**] [**version version-number**] [**source-ip {ip-address | hostname}**] [**source-port port-number**] [**cache {enable | disable}**] [**proxy proxy-url**]**
5. **frequency *seconds***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	http {get raw} <i>url</i> [name-server ip-address] [version version-number] [source-ip {ip-address hostname}] [source-port port-number] [cache {enable disable}] [proxy proxy-url] Example: Device(config-ip-sla)# http get http://198.133.219.25	Defines an HTTP operation and enters IP SLA configuration mode.
Step 5	frequency <i>seconds</i> Example: Device(config-ip-sla-http)# frequency 90	(Optional) Sets the rate at which a specified IP SLAs HTTP operation repeats. The default and minimum frequency value for an IP SLAs HTTP operation is 60 seconds.
Step 6	end Example: Device(config-ip-sla-http)# end	Exits to privileged EXEC mode.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	http {get raw} <i>url</i> [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}] [<i>proxy proxy-url</i>] Example: Device(config-ip-sla)# http get http://198.133.219.25	Defines an HTTP operation and enters IP SLA configuration mode.
Step 5	history distributions-of-statistics-kept <i>size</i> Example:	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.

	Command or Action	Purpose
	Device(config-ip-sla-http) # history distributions-of-statistics-kept 5	
Step 6	frequency seconds Example: Device(config-ip-sla-http) # frequency 90	(Optional) Sets the rate at which a specified IP SLAs HTTP operation repeats. The default and minimum frequency value for an IP SLAs HTTP operation is 60 seconds.
Step 7	history hours-of-statistics-kept hours Example: Device(config-ip-sla-http) # history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 8	http-raw-request Example: Device(config-ip-sla-http) # http-raw-request	(Optional) Explicitly specifies the options for a GET request for an IP SLAs HTTP operation.
Step 9	owner owner-id Example: Device(config-ip-sla-http) # owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 10	history statistics-distribution-interval milliseconds Example: Device(config-ip-sla-http) # history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 11	tag text Example: Device(config-ip-sla-http) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 12	threshold milliseconds Example: Device(config-ip-sla-http) # threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 13	timeout milliseconds Example: Device(config-ip-sla-http) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 14	tos number Example: Device(config-ip-sla-http) # tos 160	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 15	end Example: Device(config-ip-sla-http) # end	Exits to privileged EXEC mode.



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: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	http {get raw} <i>url</i> [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: Device(config-ip-sla)# http raw http://198.133.219.25	Defines an HTTP operation.
Step 5	http-raw-request Example: Device(config-ip-sla)# http-raw-request	Enters HTTP RAW configuration mode.

	Command or Action	Purpose
Step 6	Enter the required HTTP 1.0 command syntax. Example: Device(config-ip-sla-http)# GET /en/US/hmpgs/index.html HTTP/1.0\r\n\r\n	Specifies all the required HTTP 1.0 commands.
Step 7	end Example: Device(config-ip-sla-http)# end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month]} | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month]} | pending | now | after hh:mm [:ss]]]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: <pre>Device# show ip sla configuration</pre>	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

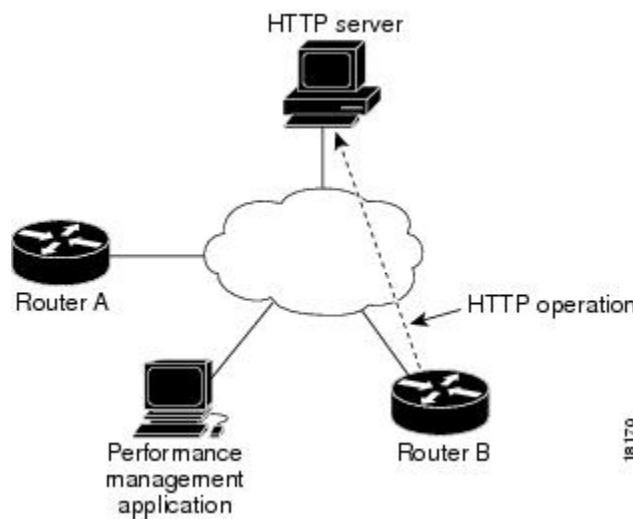
To add proactive threshold conditions and reactive triggering for generating traps (or for starting another operation) to an IP Service Level Agreements (SLAs) operation, see the “Configuring Proactive Threshold Monitoring” section.

Configuration Examples for IP SLAs HTTP Operations

Example Configuring an HTTP GET Operation

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

Figure 10: HTTP Operation



18
170

Device B Configuration

```

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

```

Example Configuring an HTTP RAW Operation

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

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

Example Configuring an HTTP RAW Operation Through a Proxy Server

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

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

Example Configuring an HTTP RAW Operation with Authentication

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

```
ip sla 8
  http raw url http://site-test.cisco.com
  http-raw-request
    GET /lab/index.html HTTP/1.0\r\n
    Authorization: Basic btNpdGT4biNvoZe=\r\n
    \r\n
    end
  ip sla schedule 8 life forever start-time now
```

Additional References

Related Documents

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

Standards and RFCs

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

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs HTTP Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 21: Feature Information for IP SLAs HTTP Operations

Feature Name	Releases	Feature Information
IP SLAs HTTP Operation		The Cisco IOS IP SLAs Hypertext Transfer Protocol (HTTP) operation allows you to measure the network response time between a Cisco device and an HTTP server to retrieve a web page.
IPSLA 4.0 - IP v6 phase2		Support was added for operability in IPv6 networks. The following commands are introduced or modified: http (IP SLA) , show ip sla configuration , show ip sla summary .
IP SLAs VRF Aware 2.0		Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 13

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, on page 185](#)
- [Information About the IP SLAs TCP Connect Operation, on page 185](#)
- [How to Configure the IP SLAs TCP Connect Operation, on page 186](#)
- [Configuration Examples for IP SLAs TCP Connect Operations, on page 192](#)
- [Additional References, on page 193](#)
- [Feature Information for the IP SLAs TCP Connect Operation, on page 194](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the IP SLAs TCP Connect Operation

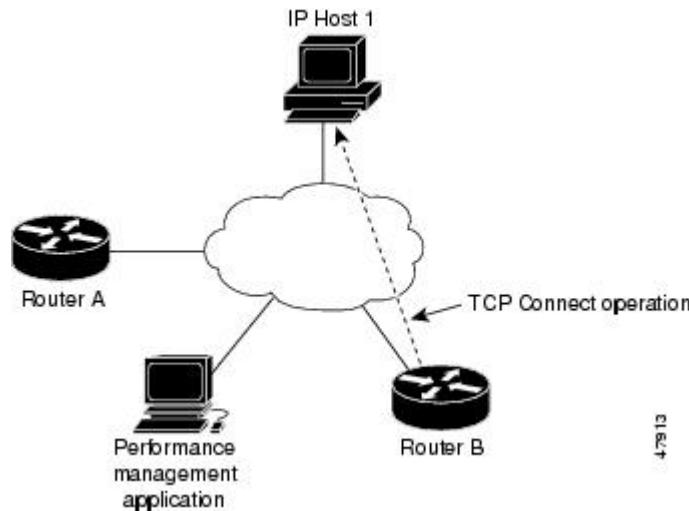
TCP Connect Operation

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

How to Configure the IP SLAs TCP Connect Operation

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

Figure 11: TCP Connect Operation



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

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

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

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

How to Configure the IP SLAs TCP Connect Operation

Configuring the IP SLAs Responder on the Destination Device

Before you begin

If you are using the IP SLAs Responder, ensure that the networking device to be used as the responder is a Cisco device and that you have connectivity to that device through the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:

- **ip sla responder**
- **ip sla responder tcp-connect ipaddress ip-address port port**

4. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Do one of the following: <ul style="list-style-type: none"> • ip sla responder • ip sla responder tcp-connect ipaddress ip-address port port Example: Device(config)# ip sla responder Example: Device(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000	(Optional) Temporarily enables IP SLAs responder functionality on the Cisco device in response to control messages from source. or (Optional) Required only if protocol control is explicitly disabled on the source device. Permanently enables IP SLAs responder functionality on the specified IP address and port. • Control is enabled by default.
Step 4	exit Example: Device(config)# exit	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a TCP Connect Operation on the Source Device

Perform only one of the following tasks:

Prerequisites

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

Configuring a Basic TCP Connect Operation on the Source Device

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	tcp-connect {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}] Example: Device(config-ip-sla)# tcp-connect 172.29.139.132 5000	Defines a TCP Connect operation and enters IP SLA TCP configuration mode. • Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target devices.
Step 5	frequency seconds Example: Device(config-ip-sla-tcp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-tcp)# end	Returns to global configuration mode.

Troubleshooting Tips

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

What to Do Next

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

operation)

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **tcp-connect {destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname} source-port port-number] [control {enable | disable}]**
5. **history buckets-kept size**
6. **history distributions-of-statistics-kept size**
7. **history enhanced [interval seconds] [buckets number-of-buckets]**
8. **history filter {none | all | overThreshold | failures}**
9. **frequency seconds**
10. **history hours-of-statistics-kept hours**
11. **history lives-kept lives**
12. **owner owner-id**
13. **history statistics-distribution-interval milliseconds**
14. **tag text**
15. **threshold milliseconds**
16. **timeout milliseconds**
17. Do one of the following:
 - **tos number**
 - **traffic-class number**
18. **flow-label number**
19. **exit**
20. **show ip sla configuration [operation-number]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	tcp-connect {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}] Example: Device(config-ip-sla)# tcp-connect 172.29.139.132 5000	Defines a TCP Connect operation and enters IP SLA TCP configuration mode. <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 devices.
Step 5	history buckets-kept size Example: Device(config-ip-sla-tcp)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	history distributions-of-statistics-kept size Example: Device(config-ip-sla-tcp)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-tcp)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter {none all overThreshold failures} Example: Device(config-ip-sla-tcp)# history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	frequency seconds Example: Device(config-ip-sla-tcp)# frequency 30	(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: Device(config-ip-sla-tcp) # history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	history lives-kept <i>lives</i> Example: Device(config-ip-sla-tcp) # history lives-kept 2	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Device(config-ip-sla-tcp) # owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	history statistics-distribution-interval <i>milliseconds</i> Example: Device(config-ip-sla-tcp) # history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	tag <i>text</i> Example: Device(config-ip-sla-tcp) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	threshold <i>milliseconds</i> Example: Device(config-ip-sla-tcp) # threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	timeout <i>milliseconds</i> Example: Device(config-ip-sla-tcp) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	Do one of the following: <ul style="list-style-type: none">• tos <i>number</i>• traffic-class <i>number</i> Example: Device(config-ip-sla-jitter) # tos 160 Example: Device(config-ip-sla-jitter) # traffic-class 160	(Optional) For IPv4: Defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) For IPv6: Defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.
Step 18	flow-label <i>number</i> Example: Device(config-ip-sla-tcp) # flow-label 112233	(Optional) For IPv6: Defines the flow label field in the IPv6 header for a supported IP SLAs operation.

	Command or Action	Purpose
Step 19	exit Example: Device(config-ip-sla-tcp)# exit	Exits TCP configuration submode and returns to global configuration mode.
Step 20	show ip sla configuration [operation-number] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Troubleshooting Tips

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

What to Do Next

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

operation)

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

Configuration Examples for IP SLAs TCP Connect Operations

Example Configuring a TCP Connect Operation

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

Device A (target device) Configuration

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

Device B (source device) Configuration

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

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

```
ip sla 9
  tcp-connect 173.29.139.132 21 control disable
  frequency 30
  ip sla schedule 9 life forever start-time now
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	<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 22: Feature Information for the IP SLAs TCP Connect Operation

Feature Name	Releases	Feature Information
IP SLAs TCP Connect Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs Transmission Control Protocol (TCP) connect operation allows you to measure the network response time taken to perform a TCP Connect operation between a Cisco device and other devices using IP.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SRC 12.2(33)SB 12.4(20)T Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG 12.2(50)SY	Support was added for operability in IPv6 networks.
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 14

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, on page 195](#)
- [Restrictions for IP SLAs ICMP Echo Operations, on page 195](#)
- [Information About IP SLAs ICMP Echo Operations, on page 196](#)
- [How to Configure IP SLAs ICMP Echo Operations, on page 196](#)
- [Configuration Examples for IP SLAs ICMP Echo Operations, on page 203](#)
- [Additional References for IP SLAs ICMP Echo Operations, on page 204](#)
- [Feature Information for IP SLAs ICMP Echo Operations, on page 204](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs ICMP Echo Operations

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

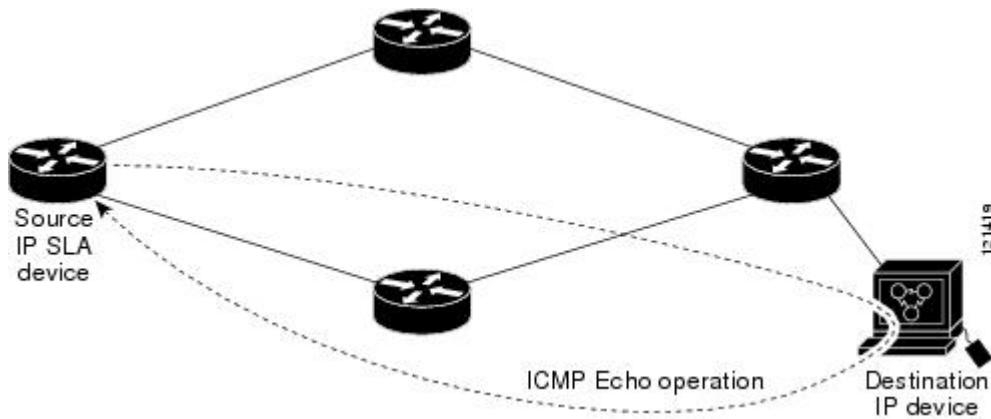
Information About IP SLAs ICMP Echo Operations

ICMP Echo Operation

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

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

Figure 12: ICMP Echo Operation



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

How to Configure IP SLAs ICMP Echo Operations

Configuring an ICMP Echo Operation



Note

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

Perform one of the following tasks:

Configuring a Basic ICMP Echo Operation on the Source Device

SUMMARY STEPS

1. `enable`
2. `configure terminal`

3. **ip sla operation-number**
4. **icmp-echo {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name]**
5. **frequency seconds**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 6	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	icmp-echo {destination-ip-address destination-hostname} [source-ip {ip-address hostname} source-interface interface-name] Example: Device(config-ip-sla)# icmp-echo 172.29.139.134	Defines an ICMP Echo operation and enters IP SLA ICMP Echo configuration mode.
Step 5	frequency seconds Example: Device(config-ip-sla-echo)# frequency 300	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-echo)# end	Exits to privileged EXEC mode.

What to do next

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

Configuring an ICMP Echo Operation with Optional Parameters

Perform this task on the source device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **icmp-echo {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name]**
5. **data-pattern hex value**
6. **history buckets-kept size**
7. **history distributions-of-statistics-kept size**
8. **history enhanced [interval seconds] [buckets number-of-buckets]**
9. **history filter {none | all | overThreshold | failures}**
10. **frequency seconds**
11. **history hours-of-statistics-kept hours**
12. **history lives-kept lives**
13. **owner owner-id**
14. **request-data-size bytes**
15. **history statistics-distribution-interval milliseconds**
16. **tag text**
17. **threshold milliseconds**
18. **timeout milliseconds**
19. Do one of the following:
 - **tos number**
 - **traffic-class number**
20. **flow-label number**
21. **verify-data**
22. **vrf vrf-name**
23. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config)# ip sla 6</pre>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	icmp-echo {destination-ip-address destination-hostname} [source-ip {ip-address hostname} source-interface interface-name] Example: Device(config-ip-sla)# icmp-echo 172.29.139.134 source-ip 172.29.139.132	Defines an Echo operation and enters IP SLA Echo configuration mode.
Step 5	data-pattern hex value Example: Device(config-ip-sla-echo)# data pattern FFFFFFFF	(Optional) Sets the hexadecimal value for data pattern. The range is 0 to FFFFFFFF.
Step 6	history buckets-kept size Example: Device(config-ip-sla-echo)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 7	history distributions-of-statistics-kept size Example: Device(config-ip-sla-echo)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 8	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-echo)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 9	history filter {none all overThreshold failures} Example: Device(config-ip-sla-echo)# history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	frequency seconds Example: Device(config-ip-sla-echo)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	history hours-of-statistics-kept hours Example: Device(config-ip-sla-echo)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.

	Command or Action	Purpose
Step 12	history lives-kept <i>lives</i> Example: Device(config-ip-sla-echo)# history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	owner <i>owner-id</i> Example: Device(config-ip-sla-echo)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	request-data-size <i>bytes</i> Example: Device(config-ip-sla-echo)# request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	history statistics-distribution-interval <i>milliseconds</i> Example: Device(config-ip-sla-echo)# history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	tag <i>text</i> Example: Device(config-ip-sla-echo)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	threshold <i>milliseconds</i> Example: Device(config-ip-sla-echo)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	timeout <i>milliseconds</i> Example: Device(config-ip-sla-echo)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	Do one of the following: <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> Example: Device(config-ip-sla-jitter)# tos 160 Example: Device(config-ip-sla-jitter)# traffic-class 160	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.

	Command or Action	Purpose
Step 20	flow-label number Example: Device(config-ip-sla-echo)# flow-label 112233	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 21	verify-data Example: Device(config-ip-sla-echo)# verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	vrf vrf-name Example: Device(config-ip-sla-echo)# vrf vpn-A	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 23	end Example: Device(config-ip-sla-echo)# end	Exits to privileged EXEC mode.

What to do next

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

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**

5. show ip sla group schedule
6. show ip sla configuration

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example:	(Optional) Displays IP SLAs group schedule details.

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

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs ICMP Echo Operations

Example Configuring an ICMP Echo Operation

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

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

Additional References for IP SLAs ICMP Echo Operations

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 862	Echo Protocol

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs ICMP Echo Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 23: Feature Information for IP SLAs ICMP Echo Operations

Feature Name	Releases	Feature Information
IP SLAs ICMP Echo Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs Internet Control Message Protocol (ICMP) echo operation allows you to measure end-to-end network response time between a Cisco device and other devices using IP.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SB 12.2(33)SRC 12.4(20)T Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG 12.2(50)SY	Support was added for operability in IPv6 networks.



CHAPTER 15

Configuring IP SLAs ICMP Path Echo Operations

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

- [Finding Feature Information, on page 207](#)
- [Restrictions for IP SLAs ICMP Path Echo Operations, on page 207](#)
- [Information About IP SLAs ICMP Path Echo Operations, on page 208](#)
- [How to Configure IP SLAs ICMP Path Echo Operations, on page 208](#)
- [Configuration Examples for IP SLAs ICMP Path Echo Operations, on page 215](#)
- [Additional References for IP SLAs ICMP Echo Operations, on page 216](#)
- [Feature Information for IP SLAs ICMP Path Echo Operations, on page 217](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs ICMP Path Echo Operations

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

Information About IP SLAs ICMP Path Echo Operations

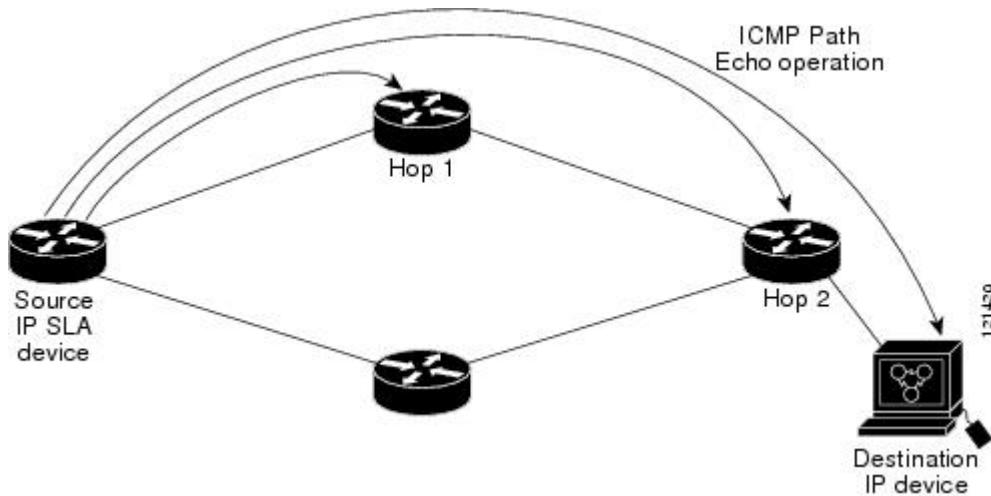
ICMP Path Echo Operation

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

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

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

Figure 13: ICMP Path Echo Operation



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

How to Configure IP SLAs ICMP Path Echo Operations

Configuring an ICMP Path Echo Operation on the Source Device



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

Perform only one of the following tasks:

Configuring a Basic ICMP Path Echo Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-id***
4. **path-echo {*destination-ip-address* | *destination-hostname*} [**source-ip {*ip-address* | *hostname*}**]**
5. **frequency *seconds***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-id</i> Example: Device(config)# ip sla 7	Specifies an ID number for the operation being configured, and enters IP SLA configuration mode.
Step 4	path-echo {<i>destination-ip-address</i> <i>destination-hostname</i>} [source-ip {<i>ip-address</i> <i>hostname</i>}] Example: Device(config-ip-sla)# path-echo 172.29.139.134	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.
Step 5	frequency <i>seconds</i> Example: Device(config-ip-sla-pathEcho)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-pathEcho)# end	Exits to privileged EXEC mode.

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

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

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	path-echo {destination-ip-address destination-hostname} [source-ip {ip-address hostname}] Example: Device(config-ip-sla)# path-echo 172.29.139.134	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.
Step 5	history buckets-kept size Example: Device(config-ip-sla-pathEcho)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	history distributions-of-statistics-kept size Example: Device(config-ip-sla-pathEcho)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-pathEcho)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter {none all overThreshold failures} Example: Device(config-ip-sla-pathEcho)# history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	frequency seconds Example: Device(config-ip-sla-pathEcho)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	history hours-of-statistics-kept hours Example:	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.

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

	Command or Action	Purpose
	Device(config-ip-sla-pathEcho) # history hours-of-statistics-kept 4	
Step 11	history lives-kept <i>lives</i> Example: Device(config-ip-sla-pathEcho) # history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Device(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: Device(config-ip-sla-pathEcho) # paths-of-statistics-kept 3	(Optional) Sets the number of paths for which statistics are maintained per hour for an IP SLAs operation.
Step 14	request-data-size <i>bytes</i> Example: Device(config-ip-sla-pathEcho) # request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	samples-of-history-kept <i>samples</i> Example: Device(config-ip-sla-pathEcho) # samples-of-history-kept 10	(Optional) Sets the number of entries kept in the history table per bucket for an IP SLAs operation.
Step 16	history statistics-distribution-interval <i>milliseconds</i> Example: Device(config-ip-sla-pathEcho) # history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 17	tag <i>text</i> Example: Device(config-ip-sla-pathEcho) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	threshold <i>milliseconds</i> Example: Device(config-ip-sla-pathEcho) # threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 19	timeout milliseconds Example: Device(config-ip-sla-pathEcho) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 20	tos number Example: Device(config-ip-sla-pathEcho) # tos 160	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 21	verify-data Example: Device(config-ip-sla-pathEcho) # verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	vrf vrf-name Example: Device(config-ip-sla-pathEcho) # vrf vpn-A	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 23	end Example: Device(config-ip-sla-pathEcho) # end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**

4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example:	(Optional) Displays IP SLAs group schedule details.

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

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

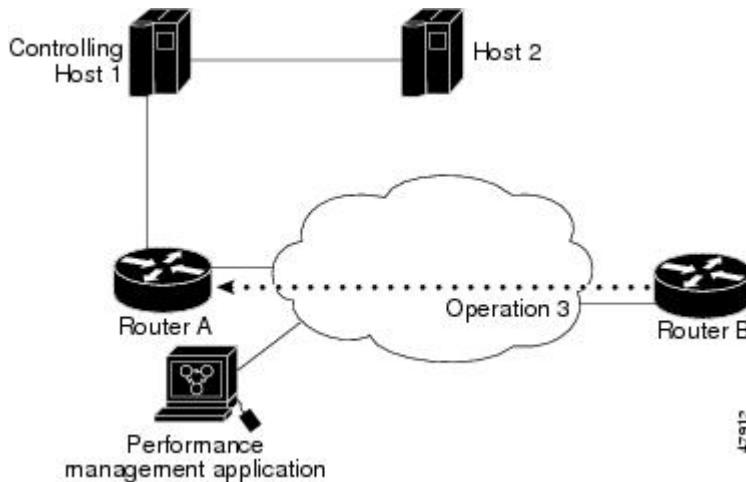
What to Do Next

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

Configuration Examples for IP SLAs ICMP Path Echo Operations

Example Configuring an ICMP Path Echo Operation

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

Figure 14: ICMP Path Echo Operation

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

Device B Configuration

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

Additional References for IP SLAs ICMP Echo Operations

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 862	Echo Protocol

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs ICMP Path Echo Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 24: Feature Information for IP SLAs ICMP Path Echo Operations

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



CHAPTER 16

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, on page 219](#)
- [Prerequisites for ICMP Path Jitter Operations, on page 219](#)
- [Restrictions for ICMP Path Jitter Operations, on page 220](#)
- [Information About IP SLAs ICMP Path Jitter Operations, on page 220](#)
- [How to Configure the IP SLAs ICMP Path Jitter Operation, on page 221](#)
- [Configuration Examples for IP SLAs ICMP Path Jitter Operations, on page 227](#)
- [Additional References, on page 228](#)
- [Feature Information for IP SLAs ICMP Path Jitter Operations, on page 229](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for ICMP Path Jitter Operations

- Before configuring any IP SLAs application, you can use the **show ip sla application** command to verify that the operation type is supported on your software image.
- In contrast with other IP SLAs operations, the IP SLAs Responder does not have to be enabled on either the target device or intermediate devices for Path Jitter operations. However, the operational efficiency may improve if you enable the IP SLAs Responder.

Restrictions for ICMP Path Jitter Operations

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

Information About IP SLAs ICMP Path Jitter Operations

ICMP Path Jitter Operation

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

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

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

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

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

How to Configure the IP SLAs ICMP Path Jitter Operation

Configuring the IP SLAs Responder on a Destination Device



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

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring an ICMP Path Jitter Operation on the Source Device

	Command or Action	Purpose
	Example: Device> enable	• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla responder Example: Device(config)# ip sla responder	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. • Control is enabled by default.
Step 4	exit Example: Device(config)# exit	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring an ICMP Path Jitter Operation on the Source Device

Perform only one of the following procedures in this section:

Configuring a Basic ICMP Path Jitter Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **path-jitter {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname}] [num-packets packet-number] [interval milliseconds] [targetOnly]**
5. **frequency seconds**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	path-jitter {destination-ip-address destination-hostname} [source-ip {ip-address hostname}] [num-packets packet-number] [interval milliseconds] [targetOnly] Example: Device(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22	Enters IP SLA Path Jitter configuration mode for configuring an ICMP Path Jitter operation.
Step 5	frequency seconds Example: Device(config-ip-sla-pathJitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-pathJitter)# end	Exits to privileged EXEC mode.

Example

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

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

Configuring an ICMP Path Jitter Operation with Additional Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **path-jitter {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname}] [num-packets packet-number] [interval milliseconds] [targetOnly]**
5. **frequency seconds**

Configuring an ICMP Path Jitter Operation with Additional Parameters

6. **owner** *owner-id*
7. **request-data-size** *bytes*
8. **tag** *text*
9. **timeout** *milliseconds*
10. **vrf** *vrf-name*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	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: Device(config-ip-sla)# path-jitter 172.31.1.129 source-ip 10.2.30.1 num-packets 12 interval 22	Enters IP SLA Path Jitter configuration mode for defining an ICMP Path Jitter operation.
Step 5	frequency <i>seconds</i> Example: Device(config-ip-sla-pathJitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	owner <i>owner-id</i> Example: Device(config-ip-sla-pathJitter)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 7	request-data-size <i>bytes</i> Example:	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.

	Command or Action	Purpose
	Device(config-ip-sla-pathJitter) # request-data-size 64	
Step 8	tag text Example: Device(config-ip-sla-pathJitter) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	timeout milliseconds Example: Device(config-ip-sla-pathJitter) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 10	vrf vrf-name Example: Device(config-ip-sla-pathJitter) # vrf vpn-A	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 11	end Example: Device(config-ip-sla-pathJitter) # end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**

5. show ip sla group schedule
6. show ip sla configuration

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example:	(Optional) Displays IP SLAs group schedule details.

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

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs ICMP Path Jitter Operations

Example Configuring a Path Jitter Operation

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

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

```

Device# configure terminal
Device(config)# ip sla 15011
Device(config-sla-monitor)# path-jitter 10.222.1.100 source-ip 10.222.3.100 num-packets 20
Device(config-sla-monitor-pathJitter)# frequency 30
Device(config-sla-monitor-pathJitter)# exit
Device(config)# ip sla schedule 15011 life forever start-time now
Device(config)# exit
Device# show ip sla statistics 15011
Round Trip Time (RTT) for Index 15011
    Latest RTT: 1 milliseconds
Latest operation start time: 15:37:35.443 EDT Mon Jun 16 2008
Latest operation return code: OK
---- Path Jitter Statistics ----
Hop IP 10.222.3.252:
Round Trip Time milliseconds:

```

Additional References

```

Latest RTT: 1 ms
Number of RTT: 20
RTT Min/Avg/Max: 1/1/3 ms
Jitter time milliseconds:
    Number of jitter: 2
    Jitter Min/Avg/Max: 2/2/2 ms
Packet Values:
    Packet Loss (Timeouts): 0
    Out of Sequence: 0
    Discarded Samples: 0
Operation time to live: Forever

```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 1889 ⁴	<i>RTP: A Transport Protocol for Real-Time Applications</i> ; see the section “Estimating the Interarrival Jitter”

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

MIBs

MIBs	MIBs Link
MIB support for the Path Jitter operation is not provided.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs ICMP Path Jitter Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 25: 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 Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE Release 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).
IPSLA 4.0 - IP v6 phase2	15.2(3)T Cisco IOS XE Release 3.7S 15.2(1)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: path-jitter , show ip sla configuration , show ip sla summary .



CHAPTER 17

Configuring IP SLAs FTP Operations

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

- [Finding Feature Information, on page 231](#)
- [Restrictions for IP SLAs FTP Operations, on page 231](#)
- [Information About IP SLAs FTP Operations, on page 232](#)
- [How to Configure IP SLAs FTP Operations, on page 233](#)
- [Configuration Examples for IP SLAs FTP Operations, on page 238](#)
- [Additional References, on page 239](#)
- [Feature Information for Configuring IP SLAs FTP Operations, on page 240](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs FTP Operations

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

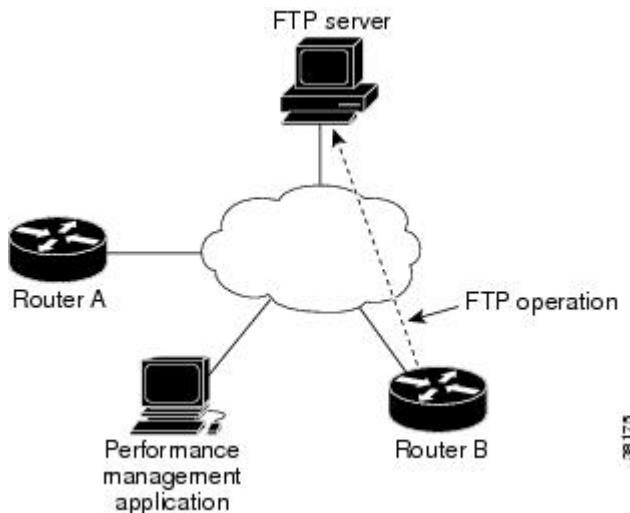
Information About IP SLAs FTP Operations

FTP Operation

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

In the figure below Device B is configured as the source IP SLAs device and an FTP operation is configured with the FTP server as the destination device.

Figure 15: FTP Operation



Connection response time is computed by measuring the time taken to download a file to Device B from the remote FTP server using FTP over TCP. This operation does not use the IP SLAs Responder.



Note To test the response time to connect to an FTP port (Port 21), use the IP SLAs TCP Connect operation.

Both active and passive FTP transfer modes are supported. The passive mode is enabled by default. Only the FTP GET (download) operation type is supported. The URL specified for the FTP GET operation must be in one of the following formats:

- `ftp://username:password@host/filename`
- `ftp://host/filename`

If the username and password are not specified, the defaults are anonymous and test, respectively.

FTP carries a significant amount of data traffic and can affect the performance of your network. The results of an IP SLAs FTP operation to retrieve a large file can be used to determine the capacity of the network but retrieve large files with caution because the FTP operation will consume more bandwidth. The FTP operation also measures your FTP server performance levels by determining the RTT taken to retrieve a file.

How to Configure IP SLAs FTP Operations

Configuring an FTP Operation on a Source Device



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

Perform one of the following tasks:

Configuring a Basic FTP Operation on the Source Device

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip sla operation-number`
4. `ftp get url [source-ip {ip-address | hostname}] [mode {passive | active}]`
5. `frequency seconds`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ftp get url [source-ip {ip-address hostname}] [mode {passive active}] Example: Device(config-ip-sla)# ftp get ftp://username:password@hostip/test.cap	Defines an FTP operation and enters IP SLA FTP configuration mode.

Configuring an FTP Operation with Optional Parameters on the Source Device

	Command or Action	Purpose
Step 5	frequency seconds Example: <pre>Device(config-ip-sla-ftp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: <pre>Device(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: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ftp get url [source-ip {ip-address hostname}] [mode {passive active}] Example: Device(config-ip-sla)# ftp get ftp://username:password@hostip/filename	Defines an FTP operation and enters IP SLA FTP configuration mode.
Step 5	history buckets-kept size Example: Device(config-ip-sla-ftp)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	history distributions-of-statistics-kept size Example: Device(config-ip-sla-ftp)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-ftp)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter {none all overThreshold failures} Example: Device(config-ip-sla-ftp)# history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	frequency seconds Example: Device(config-ip-sla-ftp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	history hours-of-statistics-kept hours Example: Device(config-ip-sla-ftp)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.

	Command or Action	Purpose
Step 11	history lives-kept <i>lives</i> Example: Device(config-ip-sla-ftp) # history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Device(config-ip-sla-ftp) # owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	history statistics-distribution-interval <i>milliseconds</i> Example: Device(config-ip-sla-ftp) # history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	tag <i>text</i> Example: Device(config-ip-sla-ftp) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	threshold <i>milliseconds</i> Example: Device(config-ip-sla-ftp) # threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	timeout <i>milliseconds</i> Example: Device(config-ip-sla-ftp) # timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	end Example: Device(config-ip-sla-ftp) # end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. enable
2. configure terminal
3. Enter one of the following commands:
 - ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]
 - ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]
4. end
5. show ip sla group schedule
6. show ip sla configuration

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

	Command or Action	Purpose
	<pre>Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	
Step 4	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: <pre>Device# show ip sla configuration</pre>	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs FTP Operations

Example: Configuring an FTP Operation

The following example shows how to configure an FTP operation from Device B to the FTP server as shown in the "FTP Operation" figure in the "Information About IP SLAs FTP Operation" section. The operation is scheduled to start every day at 1:30 a.m. In this example, the file named test.cap is to be retrieved from the host, cisco.com, with a password of abc using FTP in active mode.

Device B Configuration

```
ip sla 10
  ftp get ftp://user1:abc@test.cisco.com/test.cap mode active
  frequency 20
  tos 128
  timeout 40000
  tag FLL-FTP
ip sla schedule 10 start-time 01:30:00 recurring
```

Additional References

Related Documents

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

Feature Information for Configuring IP SLAs FTP Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 26: Feature Information for the IP SLAs FTP Operation

Feature Name	Releases	Feature Information
IP SLAs - FTP Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE Release 3.1.0SG	The IP SLAs File Transfer Protocol (FTP) operation allows you to measure the network response time between a Cisco device and an FTP server to retrieve a file.
IPSLA 4.0 - IP v6 phase2	15.2(3)T 15.2(4)S Cisco IOS XE release XE 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: ftp get (IP SLA) , show ip sla configuration , show ip sla summary .
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 18

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, on page 241](#)
- [Information About IP SLAs DNS Operations, on page 241](#)
- [How to Configure IP SLAs DNS Operations, on page 242](#)
- [Configuration Examples for IP SLAs DNS Operations, on page 248](#)
- [Additional References, on page 248](#)
- [Feature Information for Configuring IP SLAs DNS Operation, on page 249](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

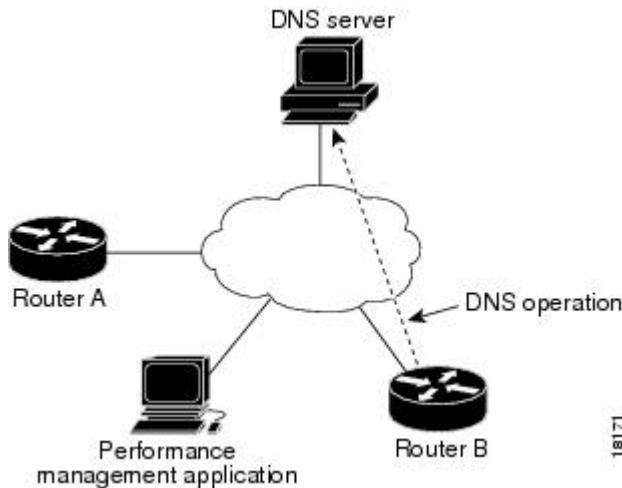
Information About IP SLAs DNS Operations

DNS Operation

The DNS operation measures the difference between the time taken to send a DNS request and receive a reply. DNS is used in the Internet for translating names of network nodes into addresses. The IP SLAs DNS operation queries for an IP address if you specify a host name, or queries for a host name if you specify an IP address.

In the figure below Device B is configured as the source IP SLAs device and a DNS operation is configured with the DNS server as the destination device.

Figure 16: DNS Operation



18171

Connection response time is computed by measuring the difference between the time taken to send a request to the DNS server and the time a reply is received by Device B. The resulting DNS lookup time can help you analyze your DNS performance. Faster DNS lookup times translate to a faster web server access experience.

How to Configure IP SLAs DNS Operations

Configuring an IP SLAs DNS Operation on the Source Device



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

Perform one of the following tasks:

Configuring a Basic DNS Operation on the Source Device

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip sla operation-number`
4. `dns {destination-ip-address | destination-hostname} name-server ip-address [source-ip {ip-address | hostname} source-port port-number]`
5. `frequency seconds`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	dns {destination-ip-address destination-hostname} name-server ip-address [source-ip {ip-address hostname} source-port port-number] Example: Device(config-ip-sla)# dns host1 name-server 172.20.2.132	Defines a DNS operation and enters IP SLA DNS configuration mode.
Step 5	frequency seconds Example: Device(config-ip-sla-dns)# frequency 60	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-dns)# end	Exits to privileged EXEC mode.

Configuring a DNS Operation with Optional Parameters on the Source Device**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **dns {destination-ip-address | destination-hostname} name-server ip-address [source-ip {ip-address | hostname} source-port port-number]**
5. **history buckets-kept size**
6. **history distributions-of-statistics-kept size**
7. **history enhanced [interval seconds] [buckets number-of-buckets]**

Configuring a DNS Operation with Optional Parameters on the Source Device

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: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Device(config)# ip sla 10</pre>	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: <pre>Device(config-ip-sla)# dns host1 name-server 172.20.2.132</pre>	Defines a DNS operation and enters IP SLA DNS configuration mode.
Step 5	history buckets-kept size Example: <pre>Device(config-ip-sla-dns)# 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	history distributions-of-statistics-kept size Example: <pre>Device(config-ip-sla-dns)# history distributions-of-statistics-kept 5</pre>	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.

	Command or Action	Purpose
Step 7	history enhanced [interval <i>seconds</i>] [buckets <i>number-of-buckets</i>] Example: Device(config-ip-sla-dns) # history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter {none all overThreshold failures} Example: Device(config-ip-sla-dns) # history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	frequency <i>seconds</i> Example: Device(config-ip-sla-dns) # frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	history hours-of-statistics-kept <i>hours</i> Example: Device(config-ip-sla-dns) # history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	history lives-kept <i>lives</i> Example: Device(config-ip-sla-dns) # history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Device(config-ip-sla-dns) # owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	history statistics-distribution-interval <i>milliseconds</i> Example: Device(config-ip-sla-dns) # history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	tag <i>text</i> Example: Device(config-ip-sla-dns) # tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
Step 15	threshold milliseconds Example: Device(config-ip-sla-dns)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	timeout milliseconds Example: Device(config-ip-sla-dns)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	end Example: Device(config-ip-sla-dns)# end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] Example: Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: Device# show ip sla configuration	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs DNS Operations

Example Configuring a DNS Operation

The following example shows how to configure a DNS operation from Device B to the DNS server (IP address 172.20.2.132) as shown in the “DNS Operation” figure in the “DNS Operation” section. The operation is scheduled to start immediately. In this example, the target address is a hostname and the DNS operation will query the DNS server for the IP address associated with the hostname host1. No configuration is required at the DNS server.

Device B Configuration

```
ip sla 11
dns host1 name-server 172.20.2.132
frequency 50
timeout 8000
tag DNS-Test
ip sla schedule 11 start-time now
```

Additional References

Related Documents

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

Related Topic	Document Title
Multioperation scheduling for IP SLAs	“Configuring Multioperation Scheduling of IP SLAs Operations” module of the <i>Cisco IOS P SLAs Configuration Guide</i>
Proactive threshold monitoring for IP SLAs	“Configuring Proactive Threshold Monitoring of IP SLAs Operations” module of the <i>Cisco IOS IP SLAs Configuration Guide</i>

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

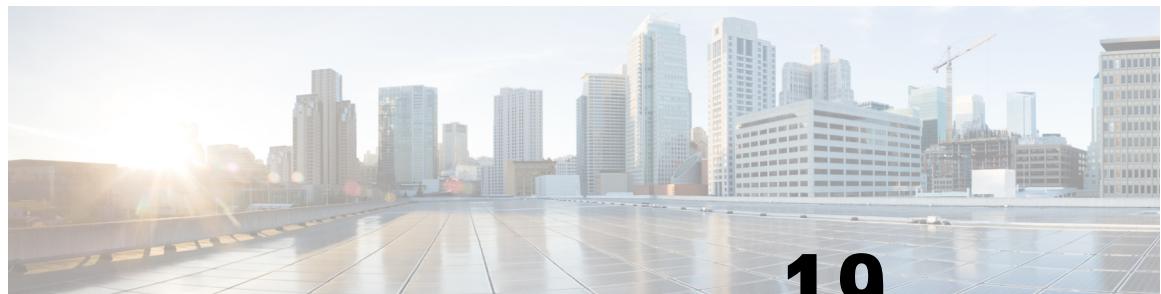
Feature Information for Configuring IP SLAs DNS Operation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 27: Feature Information for the IP SLAs - DNS Operation

Feature Name	Releases	Feature Information
IP SLAs - DNS Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG	The IP SLAs Domain Name System (DNS) Operation feature allows you to measure the difference between the time taken to send a DNS request and receive a reply.
IPSLA 4.0 - IP v6 phase2	15.2(3)T Cisco IOS XE Release 3.7S 15.1(2)SG Cisco IOS XE Release 3.4SG	Support was added for operability in IPv6 networks. The following commands are introduced or modified: dns (IP SLA) , show ip sla configuration , show ip sla summary .
IP SLAs VRF Aware 2.0	12.4(2)T 15.1(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.



CHAPTER 19

Configuring IP SLAs DHCP Operations

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

- [Finding Feature Information, on page 251](#)
- [Information About IP SLAs DHCP Operations, on page 251](#)
- [How to Configure IP SLAs DHCP Operations, on page 252](#)
- [Configuration Examples for IP SLAs DHCP Operations, on page 258](#)
- [Additional References, on page 258](#)
- [Feature Information for IP SLAs DHCP Operations, on page 259](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP SLAs DHCP Operations

DHCP Operation

DHCP provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them. The DHCP operation measures the round-trip time (RTT) taken to discover a DHCP server and obtain a leased IP address from it. IP SLAs releases the leased IP address after the operation.

You can use the RTT information to determine DHCP performance levels.

There are two modes for the DHCP operation. By default, the DHCP operation sends discovery packets on every available IP interface on the device. If a specific server is configured on the device, discovery packets are sent only to the specified DHCP server.

IP SLAs DHCP Relay Agent Options

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP device, where IP packets are switched between networks somewhat transparently. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface.

How to Configure IP SLAs DHCP Operations



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

Configuring a DHCP Operation on the Source Device

Perform one of the following tasks:

Configuring a Basic DHCP Operation

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: <pre>Device(config)# ip sla 10</pre>	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	dhcp {destination-ip-address destination-hostname} [source-ip {ip-address hostname}] Example: Device(config-ip-sla)# dhcp 10.10.10.3	Defines a DHCP operation and enters IP SLA DHCP configuration mode.
Step 5	frequency seconds Example: Device(config-ip-sla-dhcp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-dhcp)# end	Exits to privileged EXEC mode.

Configuring a DHCP Operation with Optional Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **dhcp {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname}]**
5. **history buckets-kept size**
6. **history distributions-of-statistics-kept size**
7. **history 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:	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	dhcp {destination-ip-address destination-hostname}, [source-ip {ip-address hostname}] Example: Device(config-ip-sla)# dhcp 10.10.10.3	Defines a DHCP operation and enters IP SLA DHCP configuration mode.
Step 5	history buckets-kept size Example: Device(config-ip-sla-dhcp)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	history distributions-of-statistics-kept size Example: Device(config-ip-sla-dhcp)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	history enhanced [interval seconds] [buckets number-of-buckets] Example: Device(config-ip-sla-dhcp)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter {none all overThreshold failures} Example: Device(config-ip-sla-dhcp)# history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	frequency seconds Example: Device(config-ip-sla-dhcp)# frequency 30	(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: Device(config-ip-sla-dhcp)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	history lives-kept <i>lives</i> Example: Device(config-ip-sla-dhcp)# history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Device(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: Device(config-ip-sla-dhcp)# history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	tag <i>text</i> Example: Device(config-ip-sla-dhcp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	threshold <i>milliseconds</i> Example: Device(config-ip-sla-dhcp)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	timeout <i>milliseconds</i> Example: Device(config-ip-sla-dhcp)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	end Example: Device(config-ip-sla-dhcp)# end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life 	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

	Command or Action	Purpose
	<pre>{forever seconds} [start-time {hh:mm [:ss] [month day day month]} pending now after hh:mm [:ss]}]</pre> <p>Example:</p> <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	
Step 4	end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

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

Configuration Examples for IP SLAs DHCP Operations

Example Configuration for an IP SLAs DHCP Operation

In the following example, IP SLAs operation number 12 is configured as a DHCP operation enabled for DHCP server 172.16.20.3. Note that DHCP option 82 is used to specify the circuit ID.

Device B Configuration

```
ip dhcp-server 172.16.20.3
!
ip sla 12
  dhcp 10.10.10.3
  frequency 30
  timeout 5000
  tag DHCP_Test
!
ip sla schedule 12 start-time now
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference, All Releases
Cisco IOS IP SLAs: general information	“Cisco IOS IP SLAs Overview” module of the <i>Cisco IOS IP SLAs Configuration Guide</i> .
Multioperation scheduling for IP SLAs	“Configuring Multioperation Scheduling of IP SLAs Operations” module of the <i>Cisco IOS P SLAs Configuration Guide</i>
Proactive threshold monitoring for IP SLAs	“Configuring Proactive Threshold Monitoring of IP SLAs Operations” module of the <i>Cisco IOS IP SLAs Configuration Guide</i>

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

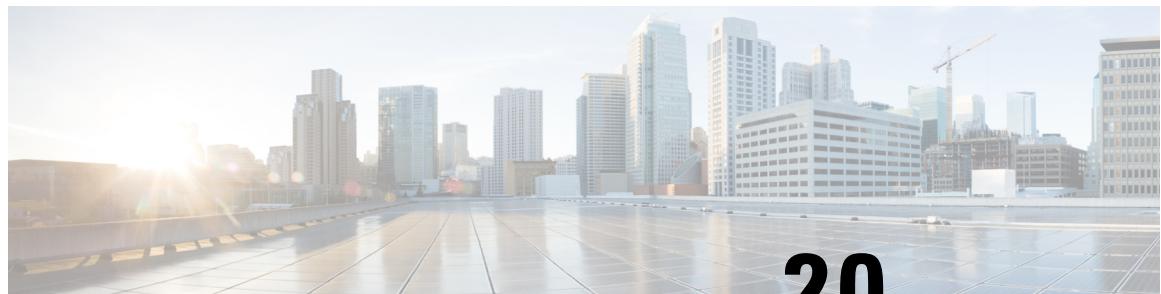
Feature Information for IP SLAs DHCP Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 28: Feature Information for IP SLAs DHCP Operations

Feature Name	Releases	Feature Information
IP SLAs DHCP Probe	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG 15.4(1)S	The IP SLAs Dynamic Host Control Protocol (DHCP) Probe feature allows you to schedule and measure the network response time between a Cisco device and a DHCP server to obtain an IP address. In Cisco IOS Release 15.4(1)S, support was added for the Cisco ASR 901S Router.



CHAPTER 20

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, on page 261](#)
- [Prerequisites, on page 261](#)
- [Information About IP SLAs DLSw+ Operations, on page 261](#)
- [How to Configure IP SLAs DLSw+ Operations, on page 262](#)
- [Configuration Examples for IP SLAs DLSw+ Operations, on page 268](#)
- [Additional References, on page 269](#)
- [Feature Information for Cisco IOS IP SLAs DLSw+ Operations, on page 270](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites

A connected DLSw+ peer between the source and destination networking devices must be configured.

Information About IP SLAs DLSw+ Operations

DLSw+ Operation

The Cisco IOS IP SLAs DLSw+ operation measures the DLSw+ protocol stack and network response time between DLSw+ peers. DLSw+ is the enhanced Cisco version of RFC 1795. DLSw+ tunnels non-routable

Layer 2 traffic such as Systems Network Architecture (SNA) traffic over IP backbones via TCP. The networking devices performing the tunneling of non-routable traffic into TCP/IP are referred to as DLSw+ peers. DLSw+ peers normally communicate through TCP port 2065. The destination networking device does not have to be a Cisco router if it supports RFC 1795.

In the figure below, Router A is configured as the source IP SLAs device and a DLSw+ operation is configured with Router B as the remote DLSw+ peer. Router A and Router B are configured as connected DLSw+ peers. The peer (destination device) does not have to run a Cisco IOS IP SLA-capable image.

Figure 17: DLSw+ Operation



Network response time is computed by measuring the round-trip time (RTT) taken to connect to the remote DLSw+ peer using TCP. This operation does not use the IP SLAs Responder.

How to Configure IP SLAs DLSw+ Operations

Configuring IP SLAs DLSw+ Operations



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

Perform one of the following tasks:

Configuring a Basic DLSw+ Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla *operation-number***
4. **dlsw peer-ipaddr *ip-address***
5. **frequency *seconds***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	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	dlsw peer-ipaddr ip-address Example: Router(config-ip-sla)# dlsw peer-ipaddr 172.21.27.11	Defines a DLSw+ operation and enters IP SLA DLSw+ configuration mode.
Step 5	frequency seconds Example: Router(config-ip-sla-dlsw)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Router(config-ip-sla-dlsw)# end	Exits to privileged EXEC mode.

Configuring an IP SLAs DLSw+ Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **dlsw peer-ipaddr ip-address**
5. **history buckets-kept size**
6. **history distributions-of-statistics-kept size**
7. **history enhanced [interval seconds] [buckets number-of-buckets]**
8. **history filter {none | all | overThreshold | failures}**
9. **frequency seconds**
10. **history hours-of-statistics-kept hours**
11. **history lives-kept lives**
12. **owner owner-id**
13. **request-data-size bytes**
14. **history statistics-distribution-interval milliseconds**
15. **tag text**

16. **threshold** *milliseconds*
17. **timeout** *milliseconds*
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Router(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	dlsw peer-ipaddr ip-address Example: Router(config-ip-sla)# dlsw peer-ipaddr 172.21.27.11	Defines a DLSw+ operation and enters IP SLA DLSw configuration mode.
Step 5	history buckets-kept size Example: Router(config-ip-sla-dlsw)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	history distributions-of-statistics-kept size Example: Router(config-ip-sla-dlsw)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	history enhanced [interval seconds] [buckets number-of-buckets] Example: Router(config-ip-sla-dlsw)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter {none all overThreshold failures} Example:	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.

	Command or Action	Purpose
	Router(config-ip-sla-dlsw)# history filter failures	
Step 9	frequency seconds Example: Router(config-ip-sla-dlsw)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	history hours-of-statistics-kept hours Example: Router(config-ip-sla-dlsw)# hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	history lives-kept lives Example: Router(config-ip-sla-dlsw)# history lives-kept 5	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner owner-id Example: Router(config-ip-sla-dlsw)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	request-data-size bytes Example: Router(config-ip-sla-dlsw)# request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 14	history statistics-distribution-interval milliseconds Example: Router(config-ip-sla-dlsw)# history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 15	tag text Example: Router(config-ip-sla-dlsw)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 16	threshold milliseconds Example: Router(config-ip-sla-dlsw)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

	Command or Action	Purpose
Step 17	timeout milliseconds Example: Router(config-ip-sla-dlsw)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 18	end Example: Router(config-ip-sla-dlsw)# exit	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]**
 - **ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range | schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm [:ss]}]**
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

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

	Command or Action	Purpose
	Device# configure terminal	
Step 3	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • ip sla schedule operation-number [life {forever seconds}] [start-time {[hh:mm:ss] [month day day month] pending now after hh:mm:ss}] [ageout seconds] [recurring] • ip sla group schedule group-operation-number operation-id-numbers {schedule-period schedule-period-range schedule-together} [ageout seconds] frequency group-operation-frequency [life {forever seconds}] [start-time {hh:mm [:ss] [month day day month] pending now after hh:mm [:ss]}] <p>Example:</p> <pre>Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre>	<ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: Device# show ip sla configuration	(Optional) Displays IP SLAs configuration details.

Troubleshooting Tips

- If the IP SLAs operation is not running and not generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use

What to Do Next

the **verify-data** command with caution during normal operations because it generates unnecessary overhead.

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

What to Do Next

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

operation)

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

Configuration Examples for IP SLAs DLSw+ Operations

Example IP SLAs DLSw+ Operation Configuration

The following example shows the configuration for a DLSw+ operation from Router A to Router B, a remote DLSw+ peer. Router B is configured as a DLSw+ peer and Router A is specified as the remote (connected) DLSw+ peer. Router A is then configured as a DLSw+ peer with Router B as the connected DLSw+ peer, and the IP SLAs DLSw+ operation parameters are configured. The operation is scheduled to start immediately and run for 7200 seconds (2 hours).

Router B Configuration

```
configure terminal
dlsw local-peer peer-id 172.21.27.11
dlsw remote-peer 0 tcp 172.20.26.10
```

Router A Configuration

```
dlsw local-peer peer-id 172.20.26.10
dlsw remote-peer 0 tcp 172.21.27.11
ip sla 14
  dlsw peer-ipaddr 172.21.27.11
  frequency 50
  timeout 50000
  tag DLSw-Test
  exit
ip sla schedule 14 life 7200 start-time now
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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

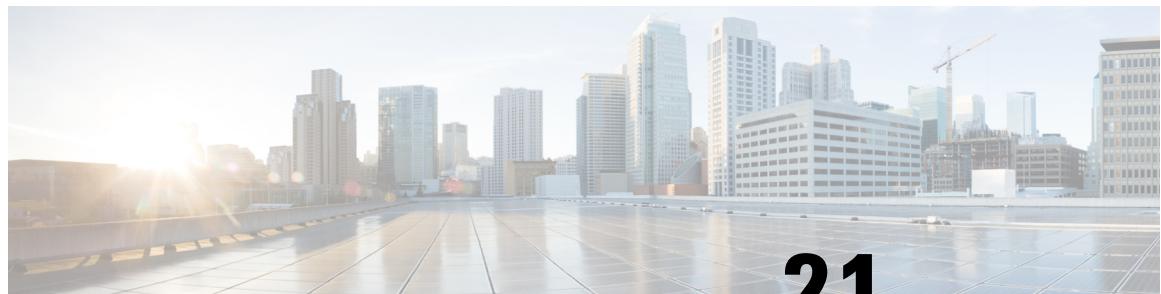
Feature Information for Cisco IOS IP SLAs DLSw+ Operations

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 29: Feature Information for Cisco IOS IP SLAs DLSw+ Operations

Feature Name	Releases	Feature Information
IP SLAs DLSw+ Operation	12.3(14)T 15.0(1)S	The Cisco IOS IP SLAs Data Link Switching Plus (DLSw+) operation allows you to schedule and measure the DLSw+ protocol stack and network response time between DLSw+ peers



CHAPTER 21

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, on page 271](#)
- [Restrictions for an IP SLAs Multioperation Scheduler, on page 271](#)
- [Prerequisites for an IP SLAs Multioperation Scheduler, on page 271](#)
- [Information About an IP SLAs Multioperation Scheduler, on page 272](#)
- [How to Configure an IP SLAs Multioperation Scheduler, on page 279](#)
- [Configuration Examples for an IP SLAs Multioperation Scheduler, on page 283](#)
- [Additional References, on page 284](#)
- [Feature Information for a IP SLAs Multioperation Scheduler, on page 284](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for an IP SLAs Multioperation Scheduler

Do not use the **no ip sla group schedule** and **ip sla group schedule** commands consecutively in a configuration file and copy it into the running configuration. This causes some of the Service Level Agreement (SLA) probes to go down.

Prerequisites for an IP SLAs Multioperation Scheduler

- Configure the IP SLAs operations to be included in a group before scheduling the group.
- Determine the IP SLAs operations you want to schedule as a single group.

Information About an IP SLAs Multioperation Scheduler

- Identify the network traffic type and the location of your network management station.
- Identify the topology and the types of devices in your network.
- Decide on the frequency of testing for each operation.

Information About an IP SLAs Multioperation Scheduler

IP SLAs Multioperations Scheduler

Normal scheduling of IP SLAs operations allows you to schedule one operation at a time. If you have large networks with thousands of IP SLAs operations to monitor network performance, normal scheduling (scheduling each operation individually) will be inefficient and time-consuming.

Multiple operations scheduling allows you to schedule multiple IP SLAs operations using a single command through the command line interface (CLI) or the CISCO-RTTMON-MIB. This feature allows you to control the amount of IP SLAs monitoring traffic by scheduling the operations to run at evenly distributed times. You must specify the operation ID numbers to be scheduled and the time range over which all the IP SLAs operations should start. This feature automatically distributes the IP SLAs operations at equal intervals over a specified time frame. The spacing between the operations (start interval) is calculated and the operations are started. This distribution of IP SLAs operations helps minimize the CPU utilization and thereby enhances the scalability of the network.

The IP SLAs multiple operations scheduling functionality allows you to schedule multiple IP SLAs operations as a group, using the following configuration parameters:

- Group operation number--Group configuration or group schedule number of the IP SLAs operation to be scheduled.
- Operation ID numbers--A list of IP SLAs operation ID numbers in the scheduled operation group.
- Schedule period--Amount of time for which the IP SLAs operation group is scheduled.
- Ageout--Amount of time to keep the operation in memory when it is not actively collecting information. By default, the operation remains in memory indefinitely.
- Frequency--Amount of time after which each IP SLAs operation is restarted. When the frequency option is specified, it overwrites the operation frequency of all operations belonging to the group. Note that when the frequency option is not specified, the frequency for each operation is set to the value of the schedule period.
- Life--Amount of time the operation actively collects information. The operation can be configured to run indefinitely. By default, the lifetime of an operation is one hour.
- Start time--Time when the operation starts collecting information. You can specify an operation to start immediately or at an absolute start time using hours, minutes, seconds, day, and month.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without aborting. However, this functionality skips those IP SLAs operations that are already running or those that are not configured and hence do not exist. The total number of operations will be calculated based on the number of operations specified in the command, irrespective of the number of operations that are missing or already running. The IP SLAs multiple operations scheduling functionality displays a message

showing the number of active and missing operations. However, these messages are displayed only if you schedule operations that are not configured or are already running.

A main benefit for scheduling multiple IP SLAs operations is that the load on the network is reduced by distributing the operations equally over a scheduled period. This distribution helps you to achieve more consistent monitoring coverage. To illustrate this scenario, consider configuring 60 operations to start during the same 1-second interval over a 60-second schedule period. If a network failure occurs 30 seconds after all 60 operations have started and the network is restored before the operations are due to start again (in another 30 seconds), then this failure would never be detected by any of the 60 operations. However, if the 60 operations are distributed equally at 1-second intervals over a 60-second schedule period, then some of the operations would detect the network failure. Conversely, if a network failure occurs when all 60 operations are active, then all 60 operations would fail, indicating that the failure is possibly more severe than it really is.

Operations of the same type and same frequency should be used for IP SLAs multiple operations scheduling. If you do not specify a frequency, the default frequency will be the same as that of the schedule period. The schedule period is the period of time in which all the specified operations should run.

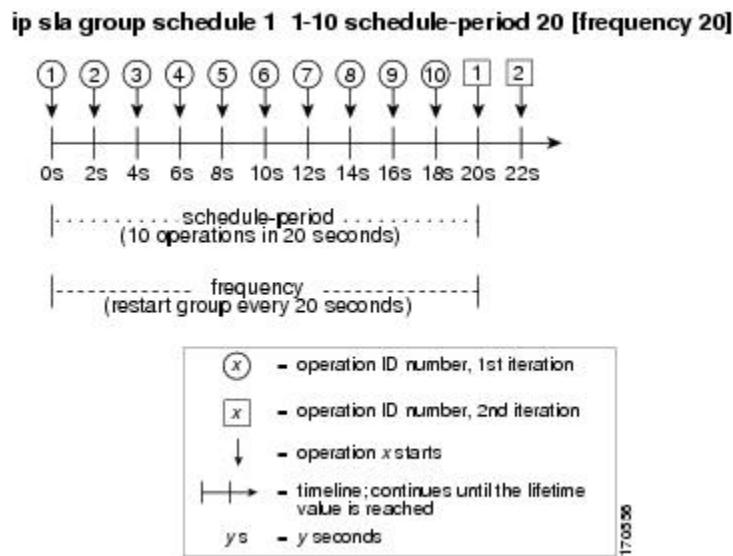
The following sections focus on the interaction of the schedule period and frequency values, additional values, such as start time and lifetime values, are not included in the illustrations.

Default Behavior of IP SLAs Multiple Operations Scheduling

The IP SLAs Multiple Operations Scheduling feature allows you to schedule multiple IP SLAs operations as a group.

The figure below illustrates the scheduling of operation group 1 that includes operation 1 to operation 10. Operation group 1 has a schedule period of 20 seconds, which means that all operations in the group will be started at equal intervals within a 20-second period. By default, the frequency is set to the same value as the configured schedule period. As shown in the figure below, configuring the frequency is optional because 20 is the default.

Figure 18: Schedule Period Equals Frequency--Default Behavior



In this example, the first operation (operation 1) in operation group 1 will start at 0 seconds. All 10 operations in operation group 1 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule

IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency

period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

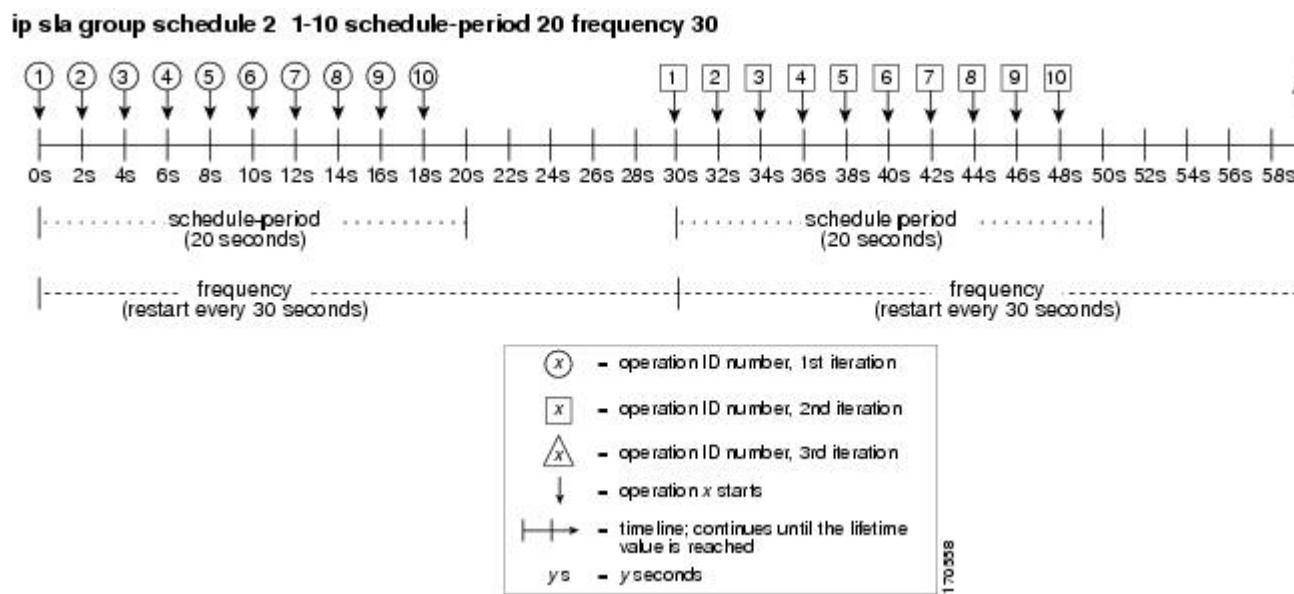
The frequency is the period of time that passes before the operation group is started again (repeated). If the frequency is not specified, the frequency is set to the value of the schedule period. In the example shown above, operation group 1 will start again every 20 seconds. This configuration provides optimal division (spacing) of operations over the specified schedule period.

IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency

The frequency value is the amount of time that passes before the schedule group is restarted, if the schedule period is less than the frequency, there will be a period of time in which no operations are started.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 2. Operation group 2 has a schedule period of 20 seconds and a frequency of 30 seconds.

Figure 19: Schedule Period Is Less Than Frequency



In this example, the first operation (operation 1) in operation group 2 will start at 0 seconds. All 10 operations in operation group 2 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

In the first iteration of operation group 2, operation 1 starts at 0 seconds, and the last operation (operation 10) starts at 18 seconds. However, because the group frequency has been configured to 30 seconds each operation in the operation group is restarted every 30 seconds. So, after 18 seconds, there is a gap of 10 seconds as no operations are started in the time from 19 seconds to 29 seconds. Hence, at 30 seconds, the second iteration of operation group 2 starts. As all ten operations in the operation group 2 must start at an evenly distributed interval in the configured schedule period of 20 seconds, the last operation (operation 10) in the operation group 2 will always start 18 seconds after the first operation (operation 1).

As illustrated in the figure above, the following events occur:

- At 0 seconds, the first operation (operation 1) in operation group 2 is started.

- At 18 seconds, the last operation (operation 10) in operation group 2 is started. This means that the first iteration (schedule period) of operation group 1 ends here.
- From 19 to 29 seconds, no operations are started.
- At 30 seconds, the first operation (operation 1) in operation group 2 is started again. The second iteration of operation group 2 starts here.
- At 48 seconds (18 seconds after the second iteration started) the last operation (operation 10) in operation group 2 is started, and the second iteration of operation group 2 ends.
- At 60 seconds, the third iteration of operation group 2 starts.

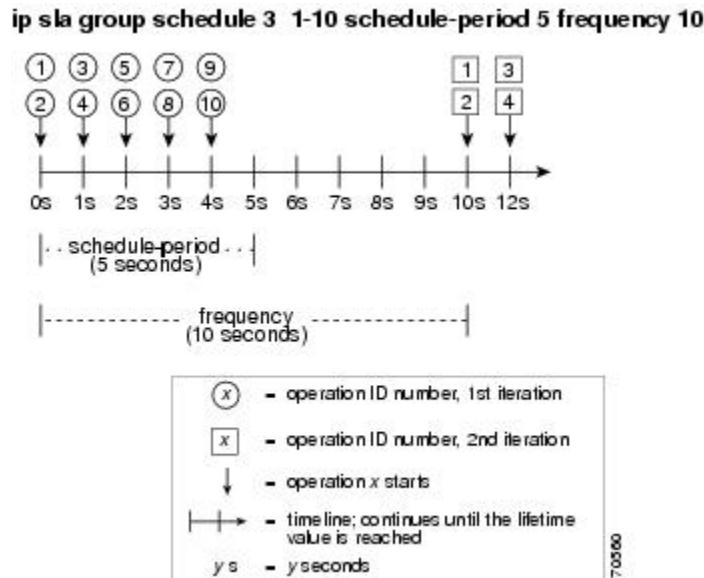
This process continues until the lifetime of operation group 2 ends. The lifetime value is configurable. The default lifetime for an operation group is forever.

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

The minimum time interval between the start of IP SLAs operations in a group operation is 1 second. Therefore, if the number of operations to be multiple scheduled is greater than the schedule period, the IP SLAs multiple operations scheduling functionality will schedule more than one operation to start within the same 1-second interval. If the number of operations getting scheduled does not equally divide into 1-second intervals, then the operations are equally divided at the start of the schedule period with the remaining operations to start at the last 1-second interval.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 3. Operation group 3 has a schedule period of 5 seconds and a frequency of 10 seconds.

Figure 20: Number of IP SLAs Operations Is Greater Than the Schedule Period--Even Distribution



In this example, when dividing the schedule period by the number of operations (5 seconds divided by 10 operations, which equals one operation every 0.5 seconds) the start time of each IP SLAs operation is less than 1 second. Since the minimum time interval between the start of IP SLAs operations in a group operation is 1 second, the IP SLAs multiple operations scheduling functionality instead calculates how many operations

IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency

it should start in each 1-second interval by dividing the number of operations by the schedule period (10 operations divided by 5 seconds). Therefore, as shown in the figure above, two operations will be started every 1 second.

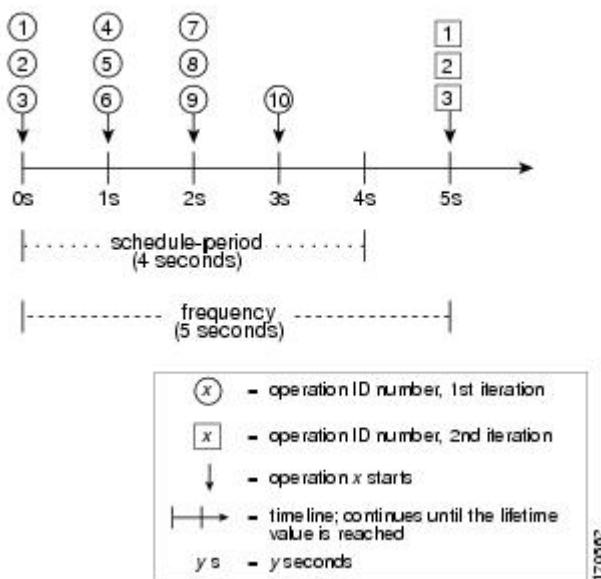
As the frequency is set to 10 in this example, each iteration of operation group 3 will start 10 seconds after the start of the previous iteration. However, this distribution is not optimal as there is a gap of 5 seconds (frequency minus schedule period) between the cycles.

If the number of operations getting scheduled does not equally divide into 1-second intervals, then the operations are equally divided at the start of the schedule period with the remaining operations to start at the last 1-second interval.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 4. Operation group 4 has a schedule period of 4 seconds and a frequency of 5 seconds.

Figure 21: Number of IP SLAs Operations Is Greater Than the Schedule Period--Uneven Distribution

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.

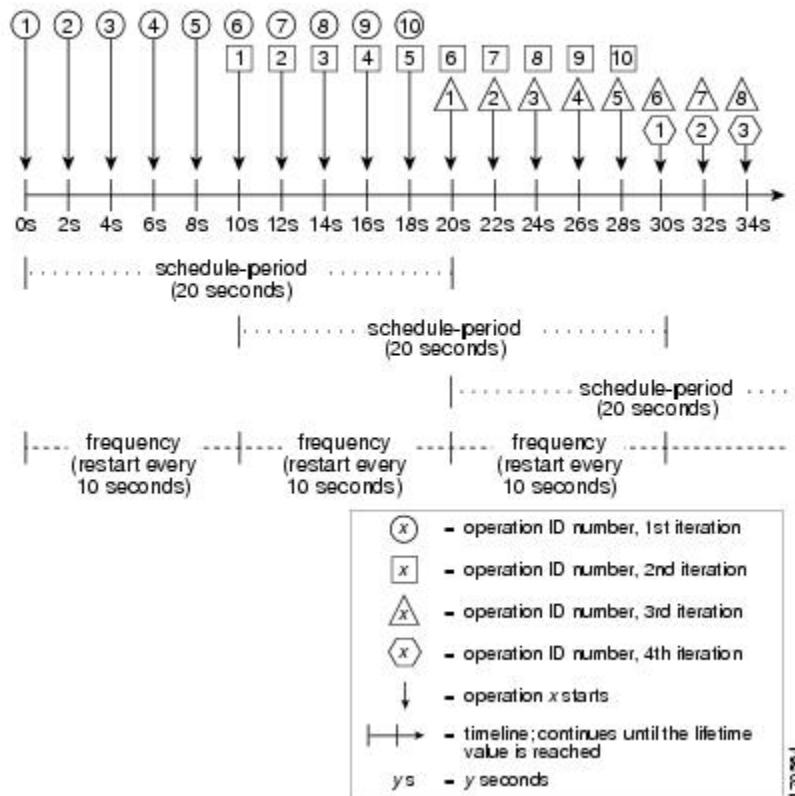
IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency

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 SLAs Group Scheduling with Schedule Period Greater Than Frequency

```
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


Note

- All IP SLAs operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group should be the same.
- List of one or more operation ID numbers to be added to a multioperation group is limited to a maximum of 125 characters, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla group schedule** *group-operation-number operation-id-numbers schedule-period schedule-period-range [ageout seconds] [frequency group-operation-frequency] [life {forever | seconds}] [start-time {hh:mm[:ss] [month day | day month] | pending | now | after hh:mm:ss}]*
4. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla group schedule <i>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}]</i> Example: Device(config)# ip sla group schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100	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	exit Example: Device(config)# exit	Returns to the privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays the IP SLAs group schedule details.
Step 6	show ip sla configuration Example: Device# show ip sla configuration	(Optional) Displays the IP SLAs configuration details.

Enabling the IP SLAs Random Scheduler

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla group schedule *group-operation-number* *operation-id-numbers* **schedule-period** *seconds* [**ageout** *seconds*] [**frequency** [*seconds*] **range** *random-frequency-range*] [**life** {**forever** | *seconds*}] [**start-time**{*hh:mm[:ss]* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]]**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla group schedule <i>group-operation-number</i> <i>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>}]]	Specifies the scheduling parameters of a group of IP SLAs operations. • To enable the IP SLAs random scheduler option, you must configure the frequency range <i>random-frequency-range</i> keywords and argument.

	Command or Action	Purpose
	Example: <pre>Device(config)# ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100</pre>	
Step 4	exit Example: <pre>Device(config)# exit</pre>	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: <pre>Device# show ip sla statistics</pre>	(Optional) Displays the IP SLAs operation details.
Step 2	show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 3	show ip sla configuration Example: <pre>Device# show ip sla configuration</pre>	(Optional) Displays the IP SLAs configuration details.

Examples

After you have scheduled the multiple IP SLAs operations, you can verify the latest operation details using the appropriate **show** commands.

The following example schedules IP SLAs operations 1 through 20 in the operation group 1 with a schedule period of 60 seconds and a life value of 1200 seconds. By default, the frequency is equivalent to the schedule period. In this example, the start interval is 3 seconds (schedule period divided by number of operations).

Verifying IP SLAs Multiple Operations Scheduling

```
Device# ip sla group schedule 1 1-20 schedule-period 60 life 1200
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla group schedule** command.

```
Device# show ip sla group schedule
Group Entry Number: 1
Probes to be scheduled: 1-20
Total number of probes: 20
Schedule period: 60
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla configuration** command. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE).

```
Device# show ip sla configuration 1
Entry number: 1
Owner:
Tag:
Type of operation to perform: udpEcho
Target address: 10.2.31.121
Source address: 0.0.0.0
Target port: 9001
Source port: 0
Request size (ARR data portion): 16
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Group Scheduled : TRUE
```

The following example shows the latest operation start time of the scheduled multiple IP SLAs operation, when the operations are scheduled at equal intervals, using the **show ip sla statistics** command:

```
Device# show ip sla statistics | include Latest operation start time
Latest operation start time: *03:06:21.760 UTC Tue Oct 21 2003
Latest operation start time: *03:06:24.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:27.751 UTC Tue Oct 21 2003
```

```

Latest operation start time: *03:06:30.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:33.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:36.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:39.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:42.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:45.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:48.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:51.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:54.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:57.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:00.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:03.754 UTC Tue Oct 21 2003
Latest operation start time: *03:07:06.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:09.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:12.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:15.755 UTC Tue Oct 21 2003
Latest operation start time: *03:07:18.752 UTC Tue Oct 21 2003

```

Configuration Examples for an IP SLAs Multioperation Scheduler

Example Scheduling Multiple IP SLAs Operations

The following example shows how to schedule IP SLAs operations 1 to 10 in the operation group 1 with a schedule period of 20 seconds. By default, the frequency is equivalent to the schedule period.

```
Device# ip sla group schedule 1 1-10 schedule-period 20
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla group schedule** command. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE).

```

Device# show ip sla group schedule
Multi-Scheduling Configuration:
Group Entry Number: 1
Probes to be scheduled: 1-10
Schedule period :20
Group operation frequency: 20
Multi-scheduled: TRUE

```

Example Enabling the IP SLAs Random Scheduler

The following example shows how to schedule IP SLAs operations 1 to 3 as a group (identified as group 2). In this example, the operations are scheduled to begin at uniformly distributed random intervals over a schedule period of 50 seconds. The first operation is scheduled to start immediately. The interval is chosen from the specified range upon every invocation of the probe. The random scheduler option is enabled and the uniformly distributed random frequencies at which the group of operations will restart is chosen within the range of 80-100 seconds.

```
ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100 start-time now
```

Additional References

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference, All Releases
Cisco IOS IP SLAs: general information	“Cisco IOS IP SLAs Overview” module of the <i>Cisco IOS IP SLAs Configuration Guide</i> .
Multioperation scheduling for IP SLAs	“Configuring Multioperation Scheduling of IP SLAs Operations” module of the <i>Cisco IOS P SLAs Configuration Guide</i>
Proactive threshold monitoring for IP SLAs	“Configuring Proactive Threshold Monitoring of IP SLAs Operations” module of the <i>Cisco IOS IP SLAs Configuration Guide</i>

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for a IP SLAs Multioperation Scheduler

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 30: Feature Information for IP SLAs Multioperation Scheduling

Feature Name	Releases	Feature Information
IP SLAs Multioperation Scheduler	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1S 15.0(1)S Cisco IOS XE 3.1.0SG	The IP SLAs Multioperation Scheduler feature provides a highly scalable infrastructure for IP SLAs by allowing you to schedule multiple IP SLAs operations using a single command.
IP SLAs Random Scheduler	12.2(33)SB 12.2(33)SXI 12.3(14)T Cisco IOS XE Release 2.1S Cisco IOS XE 3.1.0SG Cisco IOS XE Release 3.5S	The IP SLAs Random Scheduler feature provides the capability to schedule multiple IP SLAs operations to begin at random intervals uniformly distributed over a specified duration of time and to restart at uniformly distributed random frequencies within a specified frequency range.



CHAPTER 22

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, on page 287](#)
- [Information About Proactive Threshold Monitoring, on page 287](#)
- [How to Configure Proactive Threshold Monitoring, on page 292](#)
- [Configuration Examples for Proactive Threshold Monitoring, on page 294](#)
- [Additional References, on page 296](#)
- [Feature Information for IP SLAs Proactive Threshold Monitoring, on page 297](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Proactive Threshold Monitoring

IP SLAs Reaction Configuration

IP SLAs reactions are configured to trigger when a monitored value exceeds or falls below a specified level or when a monitored event, such as a timeout or connection loss, occurs. If IP SLAs measures too high or too low of any configured reaction, IP SLAs can generate a notification to a network management application or trigger another IP SLA operation to gather more data.

When an IP SLA operation is triggered, the (triggered) target operation starts and continues to run independently and without knowledge of the condition of the triggering operation. The target operation continues to run until

Supported Reactions by IP SLAs Operation

its life expires, as specified by the target operation's configured lifetime value. The target operation must finish its life before it can be triggered again.

In Cisco IOS Release 15.2(3) and later releases, the (triggered) target operation runs until the condition-cleared event. After which the target operation gracefully stops and the state of the target operation changes from Active to Pending so it can be triggered again.

Supported Reactions by IP SLAs Operation

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

Table 31: 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	--	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--	--	--	--	--
iaJitterDS	--	--	--	--	--	--	--	--	--	--
frameLossDS	--	--	--	--	--	--	--	--	--	--

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

Table 32: Supported Reaction Configuration, by IP SLA Operation

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
Failure	--	--	--	--	--	--	--	--	--
RTT	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTTAvg	--	--	--	--	--	--	--	--	--
timeout	Y	Y	Y	Y	--	Y	Y	Y	Y
connectionLoss	Y		Y	Y	Y	--	--	Y	--
verifyError	--	--	--	--	--	--	--	--	--
jitterSDAvg	--	--	--	--	--	--	Y	--	--
jitterAvg	--	--	--	--	--	--	Y	--	--
packetLateArrival	--	--	--	--	--	--	Y	--	--
packetOutOfSequence	--	--	--	--	--	--	Y	--	--
MaxOfPositiveSD	--	--	--	--	--	--	Y	--	--
MaxOfNegativeSD	--	--	--	--	--	--	Y	--	--
MaxOfPositiveDS	--	--	--	--	--	--	Y	--	--
MaxOfNegativeDS	--	--	--	--	--	--	Y	--	--
MOS	--	--	--	--	--	--	--	--	--

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
ICPIF	--	--	--	--	--	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--	--	--	--
iaJitterDS	--	--	Y	--	--	--	--	--	--
frameLossDS	--	--	Y	--	--	--	--	--	--
mosLQDSS	--	--	Y	--	--	--	--	--	--
mosCQDS	--	--	Y	--	--	--	--	--	--
rfactorDS	--	--	Y						
iaJitterSD	--	--	Y	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	--	--
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.

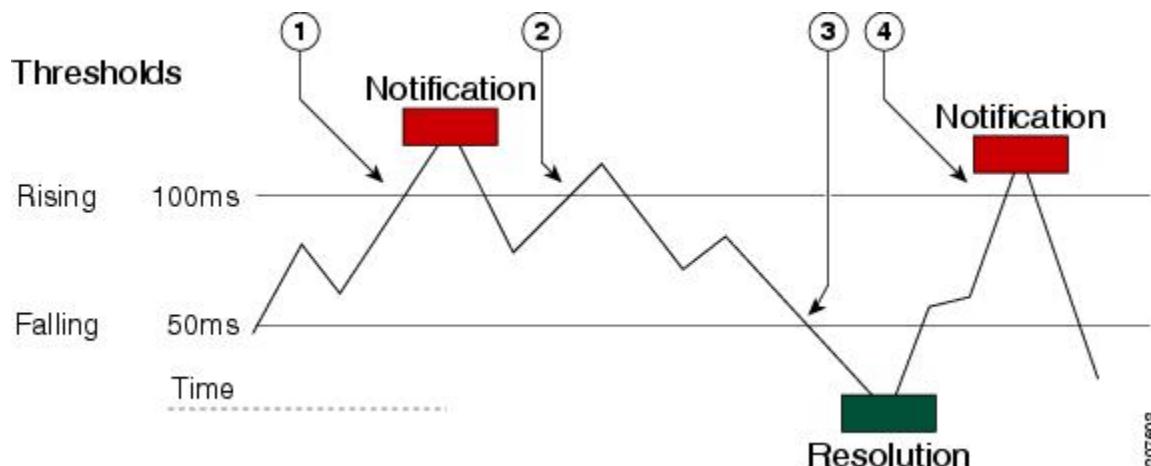
Severity levels in the CISCO-SYSLOG-MIB are defined as follows: SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)}

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: IP SLAs Triggered Reaction Condition and Notifications for Threshold Exceeded



207608

- | | |
|---|--|
| 1 | An event is sent and a threshold-exceeded notification is issued when the rising threshold is exceeded for the first time. |
| 2 | Consecutive over-rising threshold violations occur without issuing additional notifications. |
| 3 | The monitored value goes below the falling threshold. |
| 4 | Another threshold-exceeded notification is issued when the rising threshold is exceeded only after the monitored value first fell below the falling threshold. |



Note

A lower-threshold notification is also issued the first time that the monitored element falls below the falling threshold (3). As described, subsequent notifications for lower-threshold violations will be issued only after the rising threshold is exceeded before the monitored value falls below the falling threshold again.

RTT Reactions for Jitter Operations

RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT), which matches the value of the average return-trip time (RTTAvg).

SNMP traps for RTT for jitter operations are based on the value of the average return-trip time (RTTAvg) for the whole operation and do not include RTT values for each individual packet sent during the operation. For example, if the average is below the threshold, up to half of the packets can actually be above threshold but this detail is not included in the notification because the value is for the whole operation only.

Only syslog messages are supported for RTTAvg threshold violations. Syslog messages are sent from the CISCO-RTTMON-MIB.

How to Configure Proactive Threshold Monitoring

Configuring Proactive Threshold Monitoring

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

Before you begin

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



Note

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

SUMMARY STEPS

- enable**
- configure terminal**
- 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*]
- ip sla reaction-trigger** *operation-number* **target-operation**
- ip sla logging traps**
- Do one of the following:
 - snmp-server enable traps rtr**
 - snmp-server enable traps syslog**

7. **snmp-server host {hostname | ip-address} [vrf vrf-name] [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]** *community-string [udp-port port] [notification-type]*
8. **exit**
9. **show ip sla reaction- configuration [operation-number]**
10. **show ip sla reaction- trigger [operation-number]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla reaction-configuration operation-number react monitored-element [action-type option] [threshold-type {average [number-of-measurements] consecutive [occurrences] immediate never xofy [x-value y-value]}] [threshold-value upper-threshold lower-threshold] Example: Device(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger	Configures the action (SNMP trap or IP SLAs trigger) that is to occur based on violations of specified thresholds.
Step 4	ip sla reaction-trigger operation-number target-operation Example: Device(config)# ip sla reaction-trigger 10 2	(Optional) Starts another IP SLAs operation when the violation conditions are met. • Required only if the ip sla reaction-configuration command is configured with either the trapAndTrigger or triggerOnly keyword.
Step 5	ip sla logging traps Example: Device(config)# ip sla logging traps	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 6	Do one of the following: • snmp-server enable traps rtr • snmp-server enable traps syslog Example:	• (Optional) The first example shows how to enable the system to generate CISCO-RTTMON-MIB traps. • (Optional) The second example shows how to enable the system to generate CISCO-SYSLOG-MIB traps.

Configuration Examples for Proactive Threshold Monitoring

	Command or Action	Purpose
	<pre>Device(config)# snmp-server enable traps rtr</pre> Example: <pre>Device(config)# snmp-server enable traps syslog</pre>	
Step 7	<pre>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]</pre> Example: <pre>Device(config)# snmp-server host 10.1.1.1 public syslog</pre>	(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: <pre>Device(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	show ip sla reaction- configuration [operation-number] Example: <pre>Device# show ip sla reaction-configuration 10</pre>	(Optional) Displays the configuration of proactive threshold monitoring.
Step 10	show ip sla reaction- trigger [operation-number] Example: <pre>Device# show ip sla reaction-trigger 2</pre>	(Optional) Displays the configuration status and operational state of target operations to be triggered.

Configuration Examples for Proactive Threshold Monitoring

Example Configuring an IP SLAs Reaction Configuration

In the following example, IP SLAs operation 10 is configured to send an SNMP logging trap when the MOS value either exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
Device(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

The following example shows the default configuration for the **ip sla reaction-configuration** command:

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

```

Device(config)# ip sla reaction-configuration 1
Device(config)# do show ip sla reaction-configuration 1
Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None

```

Example Verifying an IP SLAs Reaction Configuration

The following example shows that multiple monitored elements are configured for the IP SLAs operation (1), as indicated by the values of Reaction: in the output:

```

Device# show ip sla reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly
Reaction: jitterDSAvg
Threshold type: immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
Reaction: PacketLossSD
Threshold type: immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly

```

Example Triggering SNMP Notifications

The following example shows how to configure proactive threshold monitoring so that CISCO-SYSLOG-MIB traps are sent to the remote host at 10.1.1.1 if the threshold values for RTT or VoIP MOS are violated:

```

! Configure the operation on source.
Device(config)# ip sla 1

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

```

Additional References

```

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

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

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

Device(config)# ip sla logging traps

! The following command sends traps to the specified remote host.
Device(config)# snmp-server host 10.1.1.1 version 2c public syslog

! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
Device(config)# snmp-server enable traps syslog

```

The following sample system logging messages shows that IP SLAs threshold violation notifications are generated as level 6 (informational) in the Cisco system logging process:

```
3d18h:%RTT-6-SAATHRESHOLD:RTR(11):Threshold exceeded for MOS
```

This following sample SNMP notification from the CISCO-SYSLOG-MIB for the same violation is a level 7 (info) notification:

```

3d18h:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 32613038
snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
clogHistoryEntry.2.71 = RTT
clogHistoryEntry.3.71 = 7
clogHistoryEntry.4.71 = SAATHRESHOLD
clogHistoryEntry.5.71 = RTR(11):Threshold exceeded for MOS
clogHistoryEntry.6.71 = 32613037

```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs Proactive Threshold Monitoring

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 33: Feature Information for IP SLAs Proactive Threshold Monitoring

Feature Name	Releases	Feature Information
IP SLAs - Reaction Threshold	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S Cisco IOS XE 3.1.0SG 12.2(50)SY	Cisco IOS IP SLAs proactive threshold monitoring capability allows you to configure an IP SLAs operation to react to certain measured network conditions.
IP SLAs - VoIP Traps	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1 15.0(1)S	The IP SLA - VoIP Traps feature includes new capabilities for configuring reaction thresholds for important VoIP related parameters such as unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring (MOS scores).

Feature Information for IP SLAs Proactive Threshold Monitoring

Feature Name	Releases	Feature Information
IP SLAs Additional Threshold Traps	12.2(33)SRB 12.2(33)SXI 12.4(2)T	This enhancement for IP SLAs reaction threshold monitoring includes per direction average jitter, per direction packet loss, maximum positive and negative jitter, and Mean Opinion Score (MOS) traps. The feature also enables one-way latency jitter, packet loss and latency traps within IP SLAs and includes traps for packet loss due to missing in action and late arrivals.



CHAPTER 23

IP SLAs TWAMP Responder

This module describes how to configure an IETF Two-Way Active Measurement Protocol (TWAMP) responder on a Cisco device to measure IP performance between the Cisco device and a non-Cisco TWAMP control device on your network.

- [Finding Feature Information, on page 299](#)
- [Prerequisites for IP SLAs TWAMP Responder, on page 299](#)
- [Restrictions for IP SLAs TWAMP Responder, on page 299](#)
- [Information About IP SLAs TWAMP Responder, on page 300](#)
- [How to Configure an IP SLAs TWAMP Responder, on page 301](#)
- [Configuration Examples for IP SLAs TWAMP Responder, on page 304](#)
- [Additional References, on page 304](#)
- [Feature Information for IP SLAs TWAMP Responder, on page 305](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP SLAs TWAMP Responder

For the IP SLAs TWAMP responder to function, a TWAMP control-client and the session-sender must be configured in your network.

Restrictions for IP SLAs TWAMP Responder

- For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector must be configured on the same Cisco device.
- Time stamping is not supported for TWAMP test packets that ingress/egress via management interface.

Information About IP SLAs TWAMP Responder

- Time stamping is not supported on interfaces that are not routed or BDI interfaces.
- Time stamping is not supported on MPLS/VPLS interfaces.
- TWAMP client and session sender is not supported.
- Up to nine session-senders can be configured for one TWAMP responder.
- TWAMP Light mode is not supported.

Information About IP SLAs TWAMP Responder

TWAMP

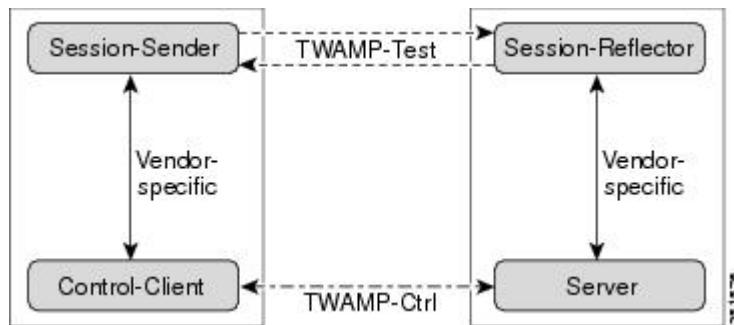
The IETF Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the TWAMP protocols. The TWAMP-Control protocol is used to set up performance measurement sessions. The TWAMP-Test protocol is used to send and receive performance-measurement probes.

The TWAMP architecture is composed of the following four logical entities that are responsible for starting a monitoring session and exchanging packets:

- The control-client sets up, starts, and stops TWAMP-Test sessions.
- The session-sender instantiates TWAMP-Test packets that are sent to the session-reflector.
- The session-reflector reflects a measurement packet upon receiving a TWAMP-Test packet. The session reflector does not collect packet statistics in TWAMP.
- The TWAMP server is an end system that manages one or more TWAMP sessions and is also capable of configuring per-session ports in the end points. The server listens on the TCP port. The session-refector and server make up the TWAMP responder in an IP SLAs operation.

Although TWAMP defines the different entities for flexibility, it also allows for logical merging of the roles on a single device for ease of implementation. The figure below shows the four entities that make up the TWAMP architecture.

Figure 24: TWAMP Architecture

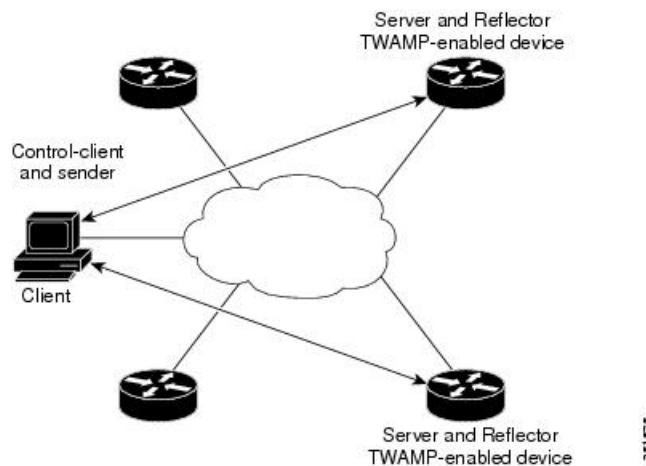


IP SLAs TWAMP Responder v1.0

A TWAMP responder interoperates with the control-client and session-sender on another device that supports TWAMP. In the IP SLAs TWAMP Responder v1.0 feature, the session-reflector and TWAMP server that make up the responder must be co-located on the same device.

In the figure below, one device is the control-client and session-sender (TWAMP control device), and the other two devices are Cisco devices that are configured as IP SLAs TWAMP responders. Each IP SLAs TWAMP responder is both a TWAMP server and a session-reflector.

Figure 25: IP SLAs TWAMP Responders in a Basic TWAMP Deployment



How to Configure an IP SLAs TWAMP Responder



Note Time stamping for sender (T1, T4) and receiver (T3, T2) is performed by hardware, instead of software to improve the accuracy of jitter and latency measurements effective Cisco IOS-XE Everest 16.6.1.

Configuring the TWAMP Server



Note For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector are configured on the same device.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip sla server twamp`
4. `port port-number`
5. `timer inactivity seconds`

6. end**DETAILED STEPS****Step 1 enable****Example:**

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 configure terminal**Example:**

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 ip sla server twamp**Example:**

```
Device(config)# ip sla server twamp
```

Configures the device as a TWAMP server and enters TWAMP server configuration mode.

Step 4 port *port-number***Example:**

```
Device(config-twamp-srvr)# port 9000
```

(Optional) Configures the port to be used by the TWAMP server to listen for connection and control requests.

Step 5 timer inactivity *seconds***Example:**

```
Device(config-twamp-srvr)# timer inactivity 300
```

(Optional) Configures the inactivity timer for a TWAMP control session.

Step 6 end**Example:**

```
Device(config-twamp-srvr)# end
```

Returns to privileged EXEC mode.

Configuring the Session-Reflector



Note For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector are configured on the same device.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip sla responder twamp
4. timeout *seconds*
5. end

DETAILED STEPS

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 ip sla responder twamp

Example:

```
Device(config)# ip sla responder twamp
```

Configures the device as a TWAMP responder and enters TWAMP reflector configuration mode.

Step 4 timeout *seconds*

Example:

```
Device(config-twamp-ref)# timeout 300
```

(Optional) Configures an inactivity timer for a TWAMP test session.

Step 5 end

Example:

```
Device(config-twamp-ref)# end
```

Exits to privileged EXEC mode.

Configuration Examples for IP SLAs TWAMP Responder

IP SLAs TWAMP Responder v1.0 Example

The following example and partial output shows how to configure the TWAMP server and the session-reflector for IP SLAs TWAMP Responder v1.0 on the same Cisco device. In this configuration, port 862 is the (default) port to be used by the TWAMP server to listen for connection and control requests. The default port for the server listener is the RFC-specified port and can be reconfigured, if required.



Note In order for the IP SLAs TWAMP responder to function, a control-client and the session-sender must be configured in your network.

```
Device> enable
Device# configure terminal
Device(config)# ip sla server twamp
Device(config-twamp-srvr)# exit
Device(config)# ip sla responder twamp
Device(config-twamp-ref)# end
Device> show running-config
.
.
.
ip sla responder
ip sla responder twamp
ip sla server twamp
port 862
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 5357	<i>Two-Way Active Measurement Protocol (TWAMP)</i>
RFC 4656	<i>One-way Active Measurement Protocol (OWAMP)</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs TWAMP Responder

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 34: Feature Information for IP SLAs TWAMP Responder

Feature Name	Releases	Feature Information
IP SLAs TWAMP Responder v1.0	15.2(2)S 15.2(3)T 15.4(1)S	<p>This feature enables you to configure the TWAMP server and the session-reflector on a Cisco device for measuring the round-trip performance between an IP SLAs TWAMP responder and a non-Cisco TWAMP control device in your network.</p> <p>The following commands were introduced or modified: ip sla responder twamp, ip sla server twamp, port (twamp), show ip sla standards, show ip sla twamp connection, show ip sla twamp session, show ip sla twamp standards, timer inactivity, timeout (twamp)..</p> <p>In Cisco IOS Release 15.4(1)S, support was added for the Cisco ASR 901S Router.</p>