



IP SLAs Configuration Guide, Cisco IOS XE Everest 3.18SP (Cisco NCS 4200 Series)

First Published: 2016-07-29

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 NON-INFRINGEMENT 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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/c/en/us/about/legal/trademarks.html>. 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)

© 2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

IP SLAs Overview 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 for Metro-Ethernet 11

- Prerequisites for IP SLAs for Metro-Ethernet 11
- Restrictions for IP SLAs for Metro-Ethernet 11
- Information About IP SLAs for Metro-Ethernet 12
 - IP SLAs Ethernet Operation Basics 12
- How to Configure IP SLAs for Metro-Ethernet 13
 - Configuring an IP SLAs Auto Ethernet Operation with Endpoint Discovery on the Source Device 13
 - Manually Configuring an IP SLAs Ethernet Ping or Jitter Operation on the Source Device 15
- Scheduling IP SLAs Operations 18
 - Troubleshooting Tips 19
 - What to Do Next 19

Configuration Examples for IP SLAs for Metro-Ethernet 20
 Example IP SLAs Auto Ethernet Operation with Endpoint Discovery 20
 Example Individual IP SLAs Ethernet Ping Operation 20
 Additional References 21

CHAPTER 3

Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 23

Prerequisites for ITU-T Y.1731 Operations 23
 Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) 23
 How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 24
 Configuring a Dual-Ended Ethernet Delay or Delay Variation Operation 24
 Configuring a Receiver MEP on the Destination Device 24
 Configuring the Sender MEP on the Source Router 27
 Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation 29
 Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation 32
 Scheduling IP SLAs Operations 35
 Enabling NTP Time of Day Synchronization 37
 Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 38
 Example: Dual-Ended Ethernet Delay Operation 38
 Example: Frame Delay and Frame Delay Variation Measurement Configuration 39
 Example: Sender MEP for a Single-Ended Ethernet Delay Operation 40
 Example: Sender MEP for a Single-Ended Ethernet Frame Loss Operation 40
 Example: Verifying NTP Time Of Day Synchronization 41
 Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 41

CHAPTER 4

Configuring an SLM 43

Configuring SLM over VPLS 43
 Restrictions for SLM support over VPLS 44
 Configuring an SLM 44
 Scheduling an IP SLA Operation 48
 Configuration Example for SLM over VPLS 50

CHAPTER 5

Configuring DMM over VPLS 51

Restrictions for DMM support over VPLS 51
 Configuring DMM over VPLS 51

Configuration Example for DMM over VPLS	52
Configuration Verification Example for DMM over VPLS	53

CHAPTER 6**IPSLA Y1731 On-Demand and Concurrent Operations 55**

Prerequisites for ITU-T Y.1731 Operations	55
Restrictions for IP SLAs Y.1731 On-Demand Operations	55
Information About IP SLAs Y.1731 On-Demand and Concurrent Operations	56
IPSLA Y1731 SLM Feature Enhancements	56
How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations	57
Configuring a Direct On-Demand Operation on a Sender MEP	57
Configuring a Referenced On-Demand Operation on a Sender MEP	58
Configuring an IP SLAs Y.1731 Concurrent Operation on a Sender MEP	58
Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations	59
Example: On-Demand Operation in Direct Mode	59
Example: On-Demand Operation in Referenced Mode	60
Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations	61

CHAPTER 7**Configuring an IP SLAs Multioperation Scheduler 63**

Prerequisites for an IP SLAs Multioperation Scheduler	63
Information About an IP SLAs Multioperation Scheduler	63
IP SLAs Multioperations Scheduler	63
Default Behavior of IP SLAs Multiple Operations Scheduling	64
IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency	65
Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period	67
IP SLAs Multiple Operations Scheduling with Scheduling Period Greater Than Frequency	68
IP SLAs Random Scheduler	70
How to Configure an IP SLAs Multioperation Scheduler	71
Scheduling Multiple IP SLAs Operations	71
Enabling the IP SLAs Random Scheduler	72
Verifying IP SLAs Multiple Operations Scheduling	73
Configuration Examples for an IP SLAs Multioperation Scheduler	75
Example Scheduling Multiple IP SLAs Operations	75
Example Enabling the IP SLAs Random Scheduler	75

[Additional References](#) 76



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).

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

Information About IP SLAs

IP SLAs Technology Overview

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

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

Depending on the specific IP SLAs operation, statistics of delay, packet loss, jitter, packet sequence, connectivity, path, server response time, and download time can be monitored within the Cisco device and

stored in both CLI and SNMP MIBs. The packets have configurable IP and application layer options such as a source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), a Virtual Private Network (VPN) routing/forwarding instance (VRF), and a URL web address.

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

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

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

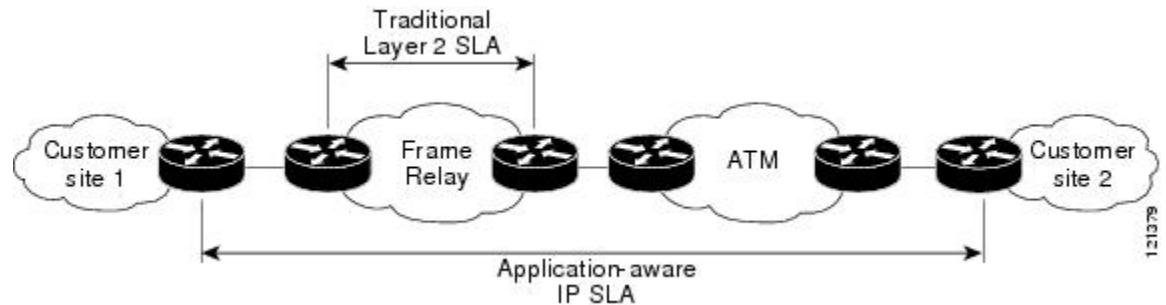
SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and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

Service Level Agreements

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

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

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



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

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

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

Benefits of IP SLAs

- IP SLAs monitoring
 - Provides service level agreement monitoring, measurement, and verification.
- Network performance monitoring
 - Measures the jitter, latency, or packet loss in the network.
 - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment
 - Verifies that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring

- Provides proactive verification and connectivity testing of network resources (for example, indicates the network availability of a Network File System (NFS) server used to store business critical data from a remote site).
- Troubleshooting of network operation
 - Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Voice over IP (VoIP) performance monitoring
- Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) performance monitoring and network verification

Restriction for IP SLAs

- With *SR_5_label_push* template, IP SLA DMM is not supported on RSP3 module.
- The maximum supported scale number of CFM and IP SLA over the port channel is only .

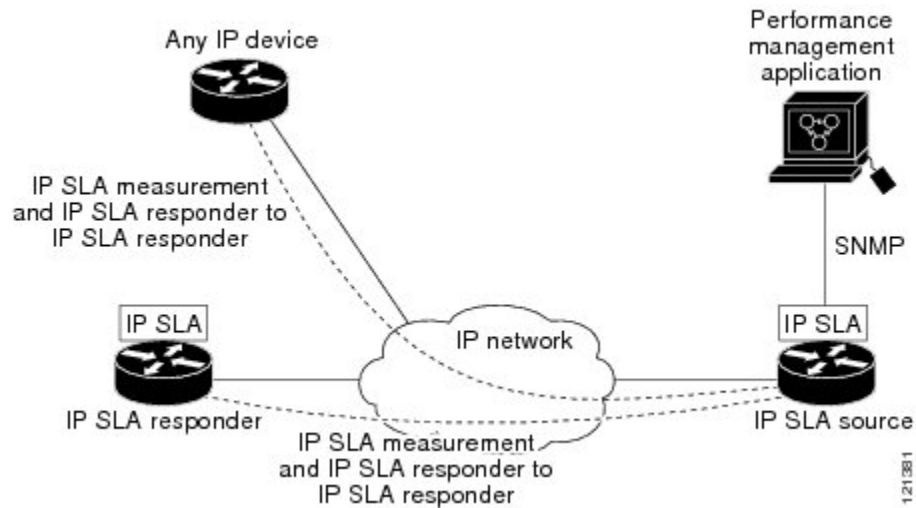
Network Performance Measurement Using IP SLAs

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,

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

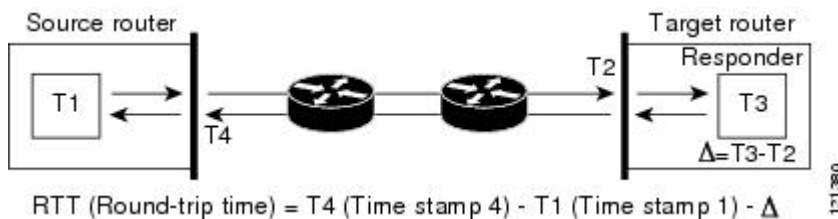
Response Time Computation for IP SLAs

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

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

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

Figure 3: IP SLAs Responder Time Stamping



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

IP SLAs Operation Scheduling

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

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

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

IP SLAs Operation Threshold Monitoring

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

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

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

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

MPLS VPN Awareness

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

History Statistics

IP SLAs maintains the following three types of history statistics:

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

- Operation snapshot history--IP SLAs maintains a snapshot of data for each operation instance that matches a configurable filter, such as all, over threshold, or failures. The entire set of data is available and no aggregation takes place.
- Distribution statistics--IP SLAs maintains a frequency distribution over configurable intervals. Each time IP SLAs starts an operation, a new history bucket is created until the number of history buckets matches the specified size or the lifetime of the operation expires. By default, the history for an IP SLAs operation is not collected. If history is collected, each bucket contains one or more history entries from the operation. History buckets do not wrap.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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



CHAPTER 2

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.

- [Prerequisites for IP SLAs for Metro-Ethernet, on page 11](#)
- [Restrictions for IP SLAs for Metro-Ethernet, on page 11](#)
- [Information About IP SLAs for Metro-Ethernet, on page 12](#)
- [How to Configure IP SLAs for Metro-Ethernet, on page 13](#)
- [Configuration Examples for IP SLAs for Metro-Ethernet, on page 20](#)
- [Additional References, on page 21](#)

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 and 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. **cos** *cos-value*
6. **owner** *owner-id*
7. **request-data-size** *bytes*
8. **tag** *text*
9. **threshold** *milliseconds*
10. **timeout** *milliseconds*
11. **end**
12. **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.
Step 4	type echo domain <i>domain-name</i> { evc <i>evc-id</i> vlan <i>vlan-id</i> } [exclude-mpids <i>mp-ids</i>]	<ul style="list-style-type: none"> • domain <i>domain-name</i>—Specify the name of the created domain.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(config-ip-sla-ethernet-monitor)# type echo domain testdomain vlan 34</pre>	<ul style="list-style-type: none"> • vlan <i>vlan-id</i>—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 <i>mp-ids</i>—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 <i>evc-id</i> keyword and argument combination may not be available for this command.</p>
Step 5	<p>cos <i>cos-value</i></p> <p>Example:</p> <pre>Device(config-ip-sla-ethernet-params)# cos 2</pre>	(Optional) Sets the class of service for an IP SLAs Ethernet operation.
Step 6	<p>owner <i>owner-id</i></p> <p>Example:</p> <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 7	<p>request-data-size <i>bytes</i></p> <p>Example:</p> <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 8	<p>tag <i>text</i></p> <p>Example:</p> <pre>Device(config-ip-sla-ethernet-params)# tag TelnetPollSever1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	<p>threshold <i>milliseconds</i></p> <p>Example:</p> <pre>Device(config-ip-sla-ethernet-params)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 10	<p>timeout <i>milliseconds</i></p> <p>Example:</p>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.

	Command or Action	Purpose
	Device(config-ip-sla-ethernet-params)# timeout 10000	
Step 11	end Example: Device(config-ip-sla-ethernet-params)# end	Exits to privileged EXEC configuration mode.
Step 12	show ip sla ethernet-monitor configuration [<i>operation-number</i>] 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Device(config)# ip sla 1	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	ethernet echo mpid <i>mp-id</i> domain <i>domain-name</i> {evc <i>evc-id</i> port vlan <i>vlan-id</i>} Example: 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 <i>evc-id</i> keyword and argument combination may not be available for this command.
Step 5	ethernet jitter mpid <i>mp-id</i> domain <i>domain-name</i> {evc <i>evc-id</i> port vlan <i>vlan-id</i>} [interval <i>interframe-interval</i>] [num-frames <i>frames-number</i>] Example: 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 <i>evc-id</i> keyword and argument combination may not be available for this command.
Step 6	cos <i>cos-value</i> Example: Device(config-ip-sla-ethernet-echo)# cos 2	(Optional) Sets the class of service for an IP SLAs Ethernet operation. Note For this and the remaining steps, the configuration mode shown in the example is for configuring an Ethernet echo operation. However, the commands are the same in the Ethernet jitter configuration mode.
Step 7	frequency <i>seconds</i> Example: Device(config-ip-sla-ethernet-echo)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
Step 8	history <i>history-parameter</i> 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 <i>owner-id</i> 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 <i>bytes</i> 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 <i>text</i> Example: Device(config-ip-sla-ethernet-echo)# tag TelnetPollSever1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 12	threshold <i>milliseconds</i> 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 <i>milliseconds</i> Example: Device(config-ip-sla-ethernet-echo)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 14	end Example: Device(config-ip-sla-ethernet-echo)# end	Exits to privileged EXEC mode.
Step 15	show ip sla configuration [<i>operation-number</i>] 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. <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	Do one of the following: <ul style="list-style-type: none"> • ip sla ethernet-monitor schedule <i>operation-number</i> schedule-period <i>seconds</i> [frequency [<i>seconds</i>]] [start-time {after <i>hh : mm : ss</i> <i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] now pending}] 	<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.

	Command or Action	Purpose
	<ul style="list-style-type: none"> ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh : mm[: ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh : mm : ss</i>}] [ageout <i>seconds</i>] [recurring] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] frequency <i>group-operation-frequency</i> [life{forever <i>seconds</i>}] [start-time{<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] <p>Example:</p> <pre>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</pre>	<ul style="list-style-type: none"> 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	<p>exit</p> <p>Example:</p> <pre>Device(config)# exit</pre>	Exits to the privileged EXEC mode.
Step 5	<p>show ip sla group schedule</p> <p>Example:</p> <pre>Device# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 6	<p>show ip sla configuration</p> <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 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 show 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> .
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



CHAPTER 3

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

- [Prerequisites for ITU-T Y.1731 Operations, on page 23](#)
- [Restrictions for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\), on page 23](#)
- [How to Configure IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations, on page 24](#)
- [Configuration Examples for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations, on page 38](#)
- [Additional References for IP SLAs Metro-Ethernet 3.0 \(ITU-T Y.1731\) Operations, on page 41](#)

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 primary PTP, and the Y1731 responder as subordinate PTP.
- 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.
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 yy 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 <i>mac-address</i> 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.

	Command or Action	Purpose
Step 6	<p>distribution {delay delay-variation} one-way <i>number-of-bins boundary[,...,boundary]</i></p> <p>Example:</p> <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	<p>frame offset <i>offset-value</i></p> <p>Example:</p> <pre>Router(config-sla-y1731-delay) # frame offset 1</pre>	(Optional) Sets the value for calculating delay variation rates.
Step 8	<p>history interval <i>intervals-stored</i></p> <p>Example:</p> <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	<p>max-delay <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-sla-y1731-delay) # max-delay 5000</pre>	(Optional) Sets the amount of time an MEP waits for a frame.
Step 10	<p>owner <i>owner-id</i></p> <p>Example:</p> <pre>Router(config-sla-y1731-delay) # owner admin</pre>	(Optional) Configures the owner of an IP SLAs operation.
Step 11	<p>end</p> <p>Example:</p> <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.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	ip sla operation-number Example: <pre>Router(config)# ip sla 500</pre>	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}}	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.

	Command or Action	Purpose
	Example: <pre>Router(config-ip-sla)# ethernet y1731 delay 1DM domain xxx evc yyy mpid 101 cos 3 source mpid 100</pre>	
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	frame interval <i>milliseconds</i> Example: <pre>Router(config-sla-y1731-delay)# frame interval 100</pre>	(Optional) Sets the gap between successive frames.
Step 7	frame size <i>bytes</i> Example: <pre>Router(config-sla-y1731-delay)# frame size 64</pre>	(Optional) Sets the padding size for frames.
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	owner <i>owner-id</i> Example: <pre>Router(config-sla-y1731-delay)# owner admin</pre>	(Optional) Configures the owner of an IP SLAs operation.
Step 10	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 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*]**
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: 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-term)# ip sla 10	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: Device(config-ip-sla)# ethernet y1731 delay dmm domain xxx evc yyy mpid 101 cos 4 source mpid 100	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: Device(config-sla-y1731-delay)# clock sync	(Optional) Indicates that the end points are synchronized and thus allows the operation to calculate one-way delay measurements.
Step 6	aggregate interval seconds 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 number-of-bins boundary[,...boundary] 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 milliseconds Example:	(Optional) Sets the gap between successive frames.

	Command or Action	Purpose
	Device(config-sla-y1731-delay)# frame interval 100	
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: Device(config-sla-y1731-delay)# owner admin	(Optional) Configures the owner of an IP SLAs operation.
Step 14	end Example: Device(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 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 This task is not supported on Cisco ME 3600X Series and 3800X Series Ethernet Access Switches



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. **ip sla reaction-configuration** *operation-number* {**react** {**unavailableDS** | **unavailableSD**} [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate**}] [**threshold-value** *upper-threshold lower-threshold*]
14. **ip sla logging traps**
15. **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 <i>operation-number</i> 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 <i>domain-name</i> { evc <i>evc-id</i> vlan <i>vlan-id</i> } { mpid <i>target-mp-id</i> mac-address <i>target-address</i> } CoS <i>CoS</i> { source { mpid <i>source-mp-id</i> mac-address <i>source-address</i> }} 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>
Step 5	aggregate interval <i>seconds</i> Example: <pre>Device(config-sla-y1731-loss)# aggregate interval 900</pre>	(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:	(Optional) Specifies availability algorithm used.

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

	Command or Action	Purpose
	Device(config-sla-y1731-loss)# availability algorithm static-window	
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: Device(config-ip-sla)# exit	Exits to global configuration mode.
Step 13	ip sla reaction-configuration <i>operation-number</i> {react {unavailableDS unavailableSD} [threshold-type {average [number-of-measurements] consecutive [occurrences] immediate}} [threshold-value upper-threshold lower-threshold] Example:	(Optional) Configures proactive threshold monitoring for frame loss measurements.

	Command or Action	Purpose
	<pre>Device(config)# ip sla reaction-configuration 11 react unavailableDS</pre>	
Step 14	<p>ip sla logging traps</p> <p>Example:</p> <pre>Device(config)# ip sla logging traps</pre>	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 15	<p>exit</p> <p>Example:</p> <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: 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	Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {[<i>hh:mm:ss</i>] [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>}] [ageout <i>seconds</i>] [recurring] • ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> {schedule-period <i>schedule-period-range</i> schedule-together} [ageout <i>seconds</i>] frequency <i>group-operation-frequency</i> [life {forever <i>seconds</i>}] [start-time {<i>hh:mm</i> [:<i>ss</i>] [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm</i> [:<i>ss</i>]}] 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.

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

Enabling NTP Time of Day Synchronization

Perform additional NTP Time Of Day synchronization configuration when NTP is chosen for time synchronization for one-way delay or delay-variation measurements on source and destination devices.



Note PTP should *not* be configured when NTP Time Of Day synchronization is used as they are mutually-exclusive configuration options for time synchronization.

For information on configuring NTP, see Configuring NTP section in [Cisco IOS Network Management Configuration Guide](#).

SUMMARY STEPS

1. enable
2. configure terminal
3. platform time-source ntp
4. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform time-source ntp Example: Router(config)# platform time-source ntp	Initiates Time of Day (ToD) synchronization on the ethernet ports.
Step 4	exit Example: Router(config)# exit	Exits the configuration.

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
```

```

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           RX Time FWD           Frame Delay
TX Time BWD           RX Time BWD           Sec:nSec
Sec:nSec              Sec:nSec              Sec:nSec
-----
Session ID: 0
*****
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
251:308856880          240:529228021          0:585

```

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

```

```

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

```

Example: Verifying NTP Time Of Day Synchronization

Use the **show platform time-source** command to display information on the time source.

```

Router# show platform time-source
Time Source mode : NTP not Configured

Router# show platform time-source
Time Source mode : NTP
NTP State          : Not Synchronized

Router# show platform time-source
Time Source mode : NTP
NTP State          : Synchronized

```

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

Related Documents

Related Topic	Document Title
Cisco IOS Carrier Ethernet commands	Cisco IOS Carrier Ethernet Command Reference
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference

Related Topic	Document Title
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



CHAPTER 4

Configuring an SLM

Synthetic loss measurement (SLM) is part of the ITU-T Y.1731 standard. It can be used to periodically measure Frame Loss and Forward Loss Ratio (FLR) between a pair of point to point MEPs. Measurements are made between two MEPs that belong to the same domain and MA.

- [Configuring SLM over VPLS, on page 43](#)
- [Restrictions for SLM support over VPLS, on page 44](#)
- [Configuring an SLM, on page 44](#)
- [Configuration Example for SLM over VPLS, on page 50](#)

Configuring SLM over VPLS

This section describes the procedure for configuring SLM over VPLS.



Note The EVC name is mandatory in the VPLS configuration methods.

SUMMARY STEPS

1. Configure CFM on PE Device
2. Configure CFM over VPLS using **l2 vfi vfi-name manual evc** command or **l2vpn vfi context vfi-name** command.
3. Configure a Sender MEP (optional task).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure CFM on PE Device	For configuration details, see Configuring Ethernet Connectivity Fault Management in a Service Provider Network . In case of H-VPLS configuration, see CFM Configuration over EFP Interface with Cross Connect Feature .
Step 2	Configure CFM over VPLS using l2 vfi vfi-name manual evc command or l2vpn vfi context vfi-name command.	The evc should be the EVC name used in the CFM on PE device configuration. For configuration details, see Configuring the VFI in the PE .

	Command or Action	Purpose
		Note The EVC name is mandatory in both the above mentioned VPLS configuration methods.
Step 3	Configure a Sender MEP (optional task).	For configuration details, see Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation .

Restrictions for SLM support over VPLS

- Only Up MEP (Maintenance End Point) on EVC (ethernet virtual circuit) BD (bridge domain) with VPLS towards the core is supported. Down MEP on VFI is not supported.
- To send unicast packets (LBR, LTM/R, Y1731 packets), port-emulation method is used. The access interface (the interface where Up MEP is configured) needs to be up to send unicast packets.
- SLM is not supported with TEF in access.
- SLM scales with frame interval of 100ms.

Configuring an SLM

To configure an SLM, execute the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal** *operation number*
3. **ip sla** *operation number*
4. **ethernet y1731 loss 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*}}
5. **aggregate interval** *seconds*
6. **availability algorithm** { **sliding-window** | **static-window** **1** } **symmetric**
7. **frame consecutive** *value*
8. **frame interval** *milliseconds*
9. **frame size** *bytes*
10. **history interval** *intervals-stored*
11. **owner** *owner-id*
12. **exit**
13. **ip sla reaction-configuration** *operation-number* [**react** {**unavailableDS** | **unavailableSD** | **loss-ratioDS** | **loss-ratioSD** }] [**threshold-type** {**average** [*number -of-measurements*] | **consecutive** [*occurrences*] | **immediate** }] [**threshold-value** *upper -threshold lower-threshold*]
14. **ip sla logging traps**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router > enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal <i>operation number</i></p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>—Identifies the IP SLAs' operation you want to configure.</p> <p>Enters global configuration mode.</p>
Step 3	<p>ip sla <i>operation number</i></p> <p>Example:</p> <pre>Router(config)# ip sla 11</pre>	<p>Configures an IP SLA operation and enters IP SLA configuration mode.</p> <ul style="list-style-type: none"> • <i>operation-number</i>—Identifies the IP SLAs' operation you want to configure.
Step 4	<p>ethernet y1731 loss SLM domain <i>domain-name</i> {evc <i>evc-id</i> vlan <i>vlan-id</i>} {mpid <i>target-mp-id</i> mac-address-target <i>-address</i>} cos <i>cos</i> {source {mpid <i>source-mp-id</i> mac-address <i>source-address</i>}}</p> <p>Example:</p> <pre>Router(config-ip-sla)# ethernet y1731 loss SLM domain xxx evc yyy mpid 101 cos 4 source mpid 100</pre>	<p>Configures a single-ended synthetic loss measurement and enters IP SLA Y.1731 loss configuration mode.</p> <ul style="list-style-type: none"> • EVC—Specifies the ethernet virtual circuit name. • SLM—Specifies that the frames sent are Synthetic Loss Measurement (SLM) frames. • domain <i>domain-name</i>—Specifies the name of the Ethernet Connectivity Fault Management (CFM) maintenance domain. • vlan <i>vlan-id</i>—Specifies the VLAN identification number. The range is from 1 to 4094. • mpid <i>target-mp-id</i>—Specifies the maintenance endpoint identification numbers of the MEP at the destination. The range is from 1 to 8191. • mac-address <i>target-address</i>—Specifies the MAC address of the MEP at the destination. • cos <i>cos</i>—Specifies, for this MEP, the class of service (CoS) that will be sent in the Ethernet message. The range is from 0 to 7. • source—Specifies the source MP ID or MAC address. • mpid <i>source-mp-id</i>—Specifies the maintenance endpoint identification numbers of the MEP being configured. The range is from 1 to 8191. • mac-address <i>source-address</i>—Specifies the MAC address of the MEP being configured.

	Command or Action	Purpose
Step 5	aggregate interval <i>seconds</i> Example: <pre>Router(config-sla-y1731-loss)# aggregate interval 900</pre>	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored. <ul style="list-style-type: none"> • <i>seconds</i>—Specifies the length of time in seconds. The range is from 1 to 65535. The default is 900.
Step 6	availability algorithm { sliding-window static-window } symmetric Example: <pre>Router(config-sla-y1731-loss)# availability algorithm static-window</pre>	(Optional) Specifies availability algorithm used. <ul style="list-style-type: none"> • sliding-window—Specifies a sliding-window control algorithm. • static-window—Specifies static-window control algorithm.
Step 7	frame consecutive <i>value</i> Example: <pre>Router(config-sla-y1731-loss)# frame consecutive 10.</pre>	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status. <ul style="list-style-type: none"> • <i>value</i>—Specifies the number of consecutive measurements. The range is from 1 to 10. The default is 10.
Step 8	frame interval <i>milliseconds</i> Example: <pre>Router(config-sla-y1731-loss)# frame interval 1000</pre>	(Optional) Sets the gap between successive frames. <ul style="list-style-type: none"> • <i>milliseconds</i>—Specifies the length of time in milliseconds (ms) between successive synthetic frames. The default is 1000
Step 9	frame size <i>bytes</i> Example: <pre>Router(config-sla-y1731-loss)# frame size 64</pre>	(Optional) Configures padding size for frames. <ul style="list-style-type: none"> • <i>bytes</i>—Specifies the padding size, in four-octet increments, for the synthetic frames. The default is 64.
Step 10	history interval <i>intervals-stored</i> Example: <pre>Router(config-sla-y1731-loss)# history interval 2</pre>	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation. <ul style="list-style-type: none"> • <i>intervals-stored</i>—Specifies the number of statistics distributions. The range is from 1 to 10. The default is 2.
Step 11	owner <i>owner-id</i> Example: <pre>Router(config-sla-y1731-loss)# owner admin</pre>	(Optional) Configures the owner of an IP SLAs operation. <ul style="list-style-type: none"> • <i>owner-id</i>—Specified the name of the SNMP owner. The value is from 0 to 255 ASCII characters.
Step 12	exit Example: <pre>Router(config-sla-y1731-loss)# exit</pre>	Exits IP SLA Y.1731 loss configuration mode and enters IP SLA configuration mode.

	Command or Action	Purpose
<p>Step 13</p>	<p>ip sla reaction-configuration <i>operation-number</i> [react {unavailableDS unavailableSD loss-ratioDS loss-ratioSD}] [threshold-type {average [<i>number-of-measurements</i>] consecutive [<i>occurrences</i>] immediate}] [threshold-value <i>upper-threshold</i> <i>lower-threshold</i>]</p> <p>Example:</p> <pre>Router(config)# ip sla reaction-configuration 11 react unavailableDS</pre>	<p>(Optional) Configures proactive threshold monitoring for frame loss measurements.</p> <ul style="list-style-type: none"> • <i>operation-number</i>—Identifies the IP SLAs operation for which reactions are to be configured. • react—(Optional) Specifies the element to be monitored for threshold violations. • unavailableDS—Specifies that a reaction should occur if the percentage of destination-to-source Frame Loss Ratio (FLR) violates the upper threshold or lower threshold. • unavailableSD—Specifies that a reaction should occur if the percentage of source-to-destination FLR violates the upper threshold or lower threshold. • loss-ratioDS—Specifies that a reaction should occur if the one-way destination-to-source loss-ratio violates the upper threshold or lower threshold. • loss-ratioSD—Specifies that a reaction should occur if the one way source-to-destination loss-ratio violates the upper threshold or lower threshold. • threshold-type average[<i>number-of-measurements</i>]—(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the action-type keyword. The default number of 5 averaged measurements can be changed using the number-of-measurements argument. The range is from 1 to 16. • threshold-type consecutive[<i>occurrences</i>]—(Optional) When a threshold violation for the monitored element is met consecutively for a specified number of times, perform the action defined by the action-type keyword. The default number of 5 consecutive occurrences can be changed using the occurrences argument. The range is from 1 to 16. • threshold-type immediate—(Optional) When a threshold violation for the monitored element is met, immediately perform the action defined by the action-type keyword. • threshold-value<i>upper-threshold</i> <i>lower-threshold</i>—(Optional) Specifies the

	Command or Action	Purpose
		upper-threshold and lower-threshold values of the applicable monitored elements.
Step 14	ip sla logging traps Example: Router(config)# ip sla logging traps	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 15	exit Example: Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.

What to do next

Once the SLM is configured, you have to schedule an IP SLA operation.

Scheduling an IP SLA Operation

To schedule an IP SLA operation, execute the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla schedule** *operation-number* [**life** { **forever** | *seconds* }] [**start-time** { *hh : mm [: ss] [month day | day month]* | **pending** | **now** | **after** *hh : mm : ss* | **random** *milliseconds* }]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters the global configuration mode.
Step 3	ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh : mm [: ss] [month day day month]</i> pending now after <i>hh : mm : ss</i> random <i>milliseconds</i> }] Example: Router(config)# ip sla schedule 10 start-time now life forever	Configures the scheduling parameters for an individual IP SLA operation or Specifies an IP SLA operation group number and the range of operation numbers to be scheduled for a multi-operation scheduler. <ul style="list-style-type: none">• <i>operation-number</i>—Identifies the IP SLAs operation for which reactions are to be configured.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • life forever— (Optional) Schedules the operation to run indefinitely. • life <i>seconds</i> —(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour). • start-time —(Optional) Time when the operation starts. • <i>hh:mm[:ss]</i>—Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, start-time 01:02 means “start at 1:02 a.m.,” and start-time 13:01:30 means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a month and day. • <i>month</i> —(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month. • <i>day</i> —(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified. • pending —(Optional) No information is collected. This is the default value. • now —(Optional) Indicates that the operation should start immediately. • after <i>hh:mm:ss</i>—(Optional) Indicates that the operation should start hh hours, mm minutes, and ss seconds after this command was entered. • random <i>milliseconds</i>—(Optional) Adds a random number of milliseconds (between 0 and the specified value) to the current time, after which the operation will start. The range is from 0 to 10000.
Step 4	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	Exits the global configuration mode and enters the privileged EXEC mode.

Configuration Example for SLM over VPLS

This section lists the CLIs and their corresponding outputs of SLM configuration over VPLS that are generated.

- **sh run | i evc**

```
ethernet evcEVC_100
```

- **sh run | sec cfm**

```
ethernet cfm global
ethernet cfm domain CFM-VPLS level 5
service ser1 evc EVC_100 vlan 100
continuity-check
continuity-check interval 1s
```

- **sh run | sec 12 vfi**

```
12 vfi VPLS-CFM manual EVC_100
vpn id 100
bridge-domain 100
neighbor 2.2.2.2 encapsulation mpls
```

- **sh run int g0/4/4**

```
interface GigabitEthernet0/4/4
service instance 100 ethernet EVC_100
encapsulation dot1q 100
```

```
cfm mep domain CFM-VPLS mpid 1001
bridge-domain 100
```

- **sh run | sec ip sla**

```
ip sla 200
ethernet y1731 loss SLM domain CFM-VPLS evc EVC_100 mpid 1002 cos 7 source mpid 1001
ip sla schedule 200 start-time now
```




CHAPTER 5

Configuring DMM over VPLS

Delay Measurement Message (DMM) is part of the ITU-T Y.1731 standard. It can be used to periodically measure Frame Delay and Frame Delay Variation between a pair of point to point MEPs. Measurements are made between two MEPs belonging to the same domain and MA.

- [Restrictions for DMM support over VPLS, on page 51](#)
- [Configuring DMM over VPLS, on page 51](#)
- [Configuration Example for DMM over VPLS, on page 52](#)

Restrictions for DMM support over VPLS

- With *SR_5_label_push* template, IP SLA DMM is not supported on RSP3 module.
- Only Up MEP(Maintenance End Point) on EVC(ethernet virtual circuit) BD(bridge domain) with VPLS towards the core is supported. Down MEP on VFI is not supported.
- To send unicast packets (LBR, LTM/R, Y1731 packets), port-emulation method is used. The access interface (the interface where Up MEP is configured) needs to be up to send unicast packets.

Configuring DMM over VPLS

SUMMARY STEPS

1. Configure CFM on PE Device.
2. Configure CFM over VPLS using **l2 vfi vfi-name manual evc** command or **l2vpn vfi context vfi-name** command.
3. Configure a Sender MEP.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure CFM on PE Device.	For configuration details see, Configuring Ethernet Connectivity Fault Management in a Service Provider Network .

	Command or Action	Purpose
		In case of H-VPLS configuration, see, CFM Configuration over EFP Interface with Cross Connect Feature .
Step 2	Configure CFM over VPLS using l2 vfi vfi-name manual evc command or l2vpn vfi context vfi-name command.	The evc should be the EVC name used in the CFM on PE device configuration. For configuration details, see, Configuring the VFI in the PE .
Step 3	Configure a Sender MEP.	For configuration details see, Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation .

Configuration Example for DMM over VPLS

The following sample output shows the configuration of DMM over VPLS:

```

ethernet evc EVC_100
ethernet cfm global
ethernet cfm domain CFM-VPLS level 5
service ser1 evc EVC_100 vlan 100
continuity-check
continuity-check interval 1s
l2 vfi VPLS-CFM manual EVC_100
vpn id 100
bridge-domain 100
neighbor 2.2.2.2 encapsulation mpls
interface GigabitEthernet0/4/4
service instance 100 ethernet EVC_100
encapsulation dot1q 100
cfm mep domain CFM-VPLS mpid 1001
bridge-domain 100
ip sla 200
ethernet y1731 delay DMM domain CFM-VPLS evc EVC_100 mpid 1002 cos 7 source mpid 1001
ip sla schedule 200 start-time now

```

The following sample output shows the configuration of DMM over VPLS using the **l2vpn vfi context** command:

```

ethernet evc EVC_100
ethernet cfm global
ethernet cfm domain CFM-VPLS level 5
service ser1 evc EVC_100 vlan 100
continuity-check
continuity-check interval 1s
l2vpn vfi context VPLS-CFM
vpn id 100
evc EVC_100
neighbor 2.2.2.2 encapsulation mpls
interface GigabitEthernet0/4/4
service instance 100 ethernet EVC_100
encapsulation dot1q 100
cfm mep domain CFM-VPLS mpid 1001
bridge-domain 100
member GigabitEthernet0/4/4 service-instance 100
member vfi VPLS-CFM
ip sla 200
ethernet y1731 delay DMM domain CFM-VPLS evc EVC_100 mpid 1002 cos 7 source mpid 1001
ip sla schedule 200 start-time now

```



Note The EVC name is mandatory and should be the same as the one configured in CFM.

Configuration Verification Example for DMM over VPLS

The following sample output shows the configuration verification of DMM over VPLS:

```

Router#sh ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 200
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: CFM_VPLS
Evc: EVC_100
Target Mpid: 1002
Source Mpid: 1001
CoS: 7
  Max Delay: 5000
  Request size (Padding portion): 64
  Frame Interval: 1000
  Clock: Not In Sync
Threshold (milliseconds): 5000
Schedule:
  Operation frequency (seconds): 900 (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): Active
Statistics Parameters
  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
  Aggregation Period: 900
History
  Number of intervals: 2

Router#

```




CHAPTER 6

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.

- [Prerequisites for ITU-T Y.1731 Operations, on page 55](#)
- [Restrictions for IP SLAs Y.1731 On-Demand Operations, on page 56](#)
- [Information About IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 56](#)
- [How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 57](#)
- [Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 59](#)
- [Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 61](#)

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 <i>domain-name</i> { evc <i>evc-id</i> vlan <i>vlan-id</i> } { mpid <i>target-mp-id</i> mac-address <i>target-address</i> } cos <i>cos</i> { source { mpid <i>source-mp-id</i> mac-address <i>source-address</i> }} { continuous [interval <i>milliseconds</i>] burst [interval <i>milliseconds</i>] [number <i>number-of-frames</i>] [frequency <i>seconds</i>]} [size <i>bytes</i>] aggregation <i>seconds</i> { duration <i>seconds</i> max <i>number-of-packets</i> }	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.

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

1. enable
2. 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 ip sla on-demand ethernet [dmmv1 slm] operation-number {duration seconds max number-of-packets} 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. <ul style="list-style-type: none"> • 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

```

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

Related Topic	Document Title
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 	<p>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Technical Assistance

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



CHAPTER 7

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.

- [Prerequisites for an IP SLAs Multioperation Scheduler, on page 63](#)
- [Information About an IP SLAs Multioperation Scheduler, on page 63](#)
- [How to Configure an IP SLAs Multioperation Scheduler, on page 71](#)
- [Configuration Examples for an IP SLAs Multioperation Scheduler, on page 75](#)
- [Additional References, on page 76](#)

Prerequisites for an IP SLAs Multioperation Scheduler

- Configure the IP SLAs operations to be included in a group before scheduling the group.
- Determine the IP SLAs operations you want to schedule as a single group.
- Identify the network traffic type and the location of your network management station.
- Identify the topology and the types of devices in your network.
- Decide on the frequency of testing for each operation.

Information About an IP SLAs Multioperation Scheduler

IP SLAs Multioperations Scheduler

Normal scheduling of IP SLAs operations allows you to schedule one operation at a time. If you have large networks with thousands of IP SLAs operations to monitor network performance, normal scheduling (scheduling each operation individually) will be inefficient and time-consuming.

Multiple operations scheduling allows you to schedule multiple IP SLAs operations using a single command through the command line interface (CLI) or the CISCO-RTTMON-MIB. This feature allows you to control the amount of IP SLAs monitoring traffic by scheduling the operations to run at evenly distributed times. You must specify the operation ID numbers to be scheduled and the time range over which all the IP SLAs operations should start. This feature automatically distributes the IP SLAs operations at equal intervals over a specified time frame. The spacing between the operations (start interval) is calculated and the operations are started.

This distribution of IP SLAs operations helps minimize the CPU utilization and thereby enhances the scalability of the network.

The IP SLAs multiple operations scheduling functionality allows you to schedule multiple IP SLAs operations as a group, using the following configuration parameters:

- Group operation number--Group configuration or group schedule number of the IP SLAs operation to be scheduled.
- Operation ID numbers--A list of IP SLAs operation ID numbers in the scheduled operation group.
- Schedule period--Amount of time for which the IP SLAs operation group is scheduled.
- Ageout--Amount of time to keep the operation in memory when it is not actively collecting information. By default, the operation remains in memory indefinitely.
- Frequency--Amount of time after which each IP SLAs operation is restarted. When the frequency option is specified, it overwrites the operation frequency of all operations belonging to the group. Note that when the frequency option is not specified, the frequency for each operation is set to the value of the schedule period.
- Life--Amount of time the operation actively collects information. The operation can be configured to run indefinitely. By default, the lifetime of an operation is one hour.
- Start time--Time when the operation starts collecting information. You can specify an operation to start immediately or at an absolute start time using hours, minutes, seconds, day, and month.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without terminating. 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.

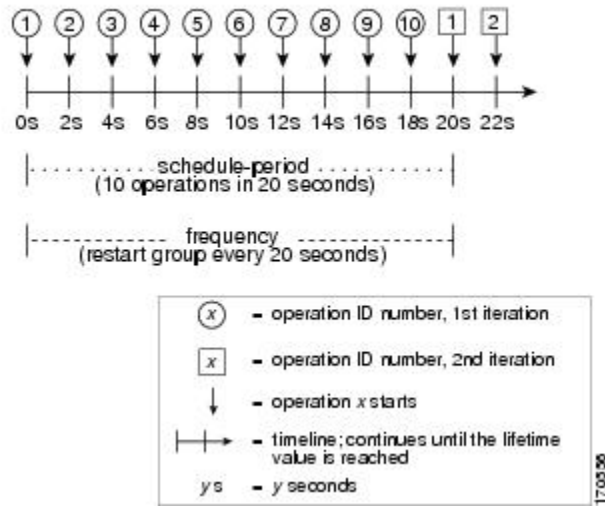
Default Behavior of IP SLAs Multiple Operations Scheduling

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 4: Schedule Period Equals Frequency--Default Behavior

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



In this example, the first operation (operation 1) in operation group 1 will start at 0 seconds. All 10 operations in operation group 1 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

The frequency is the period of time that passes before the operation group is started again (repeated). If the frequency is not specified, the frequency is set to the value of the schedule period. In the example shown above, operation group 1 will start again every 20 seconds. This configuration provides optimal division (spacing) of operations over the specified schedule period.

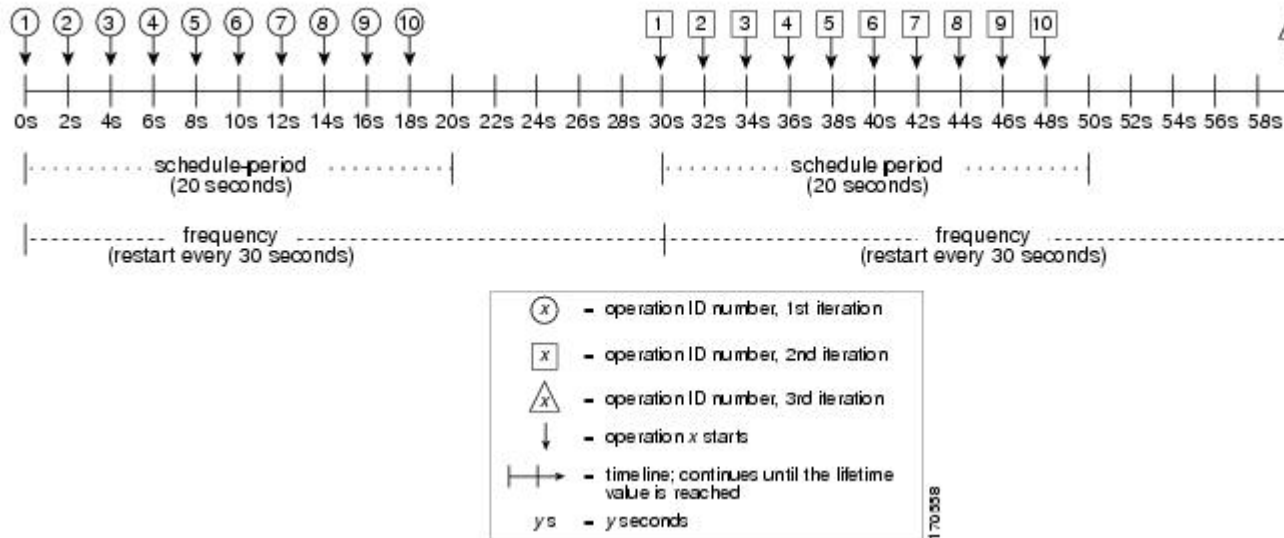
IP SLAs Multiple Operations Scheduling with Scheduling Period Less Than Frequency

The frequency value is the amount of time that passes before the schedule group is restarted, if the schedule period is less than the frequency, there will be a period of time in which no operations are started.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 2. Operation group 2 has a schedule period of 20 seconds and a frequency of 30 seconds.

Figure 5: Schedule Period Is Less Than Frequency

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



In this example, the first operation (operation 1) in operation group 2 will start at 0 seconds. All 10 operations in operation group 2 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

In the first iteration of operation group 2, operation 1 starts at 0 seconds, and the last operation (operation 10) starts at 18 seconds. However, because the group frequency has been configured to 30 seconds each operation in the operation group is restarted every 30 seconds. So, after 18 seconds, there is a gap of 10 seconds as no operations are started in the time from 19 seconds to 29 seconds. Hence, at 30 seconds, the second iteration of operation group 2 starts. As all ten operations in the operation group 2 must start at an evenly distributed interval in the configured schedule period of 20 seconds, the last operation (operation 10) in the operation group 2 will always start 18 seconds after the first operation (operation 1).

As illustrated in the figure above, the following events occur:

- At 0 seconds, the first operation (operation 1) in operation group 2 is started.
- At 18 seconds, the last operation (operation 10) in operation group 2 is started. This means that the first iteration (schedule period) of operation group 1 ends here.
- From 19 to 29 seconds, no operations are started.
- At 30 seconds, the first operation (operation 1) in operation group 2 is started again. The second iteration of operation group 2 starts here.
- At 48 seconds (18 seconds after the second iteration started) the last operation (operation 10) in operation group 2 is started, and the second iteration of operation group 2 ends.
- At 60 seconds, the third iteration of operation group 2 starts.

This process continues until the lifetime of operation group 2 ends. The lifetime value is configurable. The default lifetime for an operation group is forever.

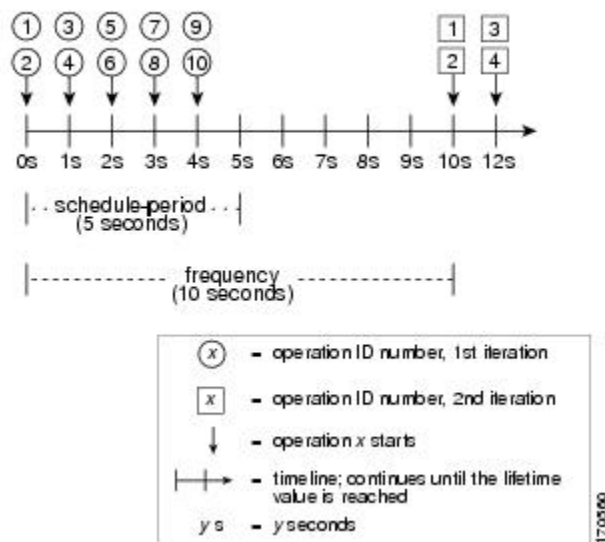
Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period

The minimum time interval between the start of IP SLAs operations in a group operation is 1 second. Therefore, if the number of operations to be multiple scheduled is greater than the schedule period, the IP SLAs multiple operations scheduling functionality will schedule more than one operation to start within the same 1-second interval. If the number of operations getting scheduled does not equally divide into 1-second intervals, then the operations are equally divided at the start of the schedule period with the remaining operations to start at the last 1-second interval.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 3. Operation group 3 has a schedule period of 5 seconds and a frequency of 10 seconds.

Figure 6: Number of IP SLAs Operations Is Greater Than the Schedule Period--Even Distribution

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



In this example, when dividing the schedule period by the number of operations (5 seconds divided by 10 operations, which equals one operation every 0.5 seconds) the start time of each IP SLAs operation is less than 1 second. Since the minimum time interval between the start of IP SLAs operations in a group operation is 1 second, the IP SLAs multiple operations scheduling functionality instead calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (10 operations divided by 5 seconds). Therefore, as shown in the figure above, two operations will be started every 1 second.

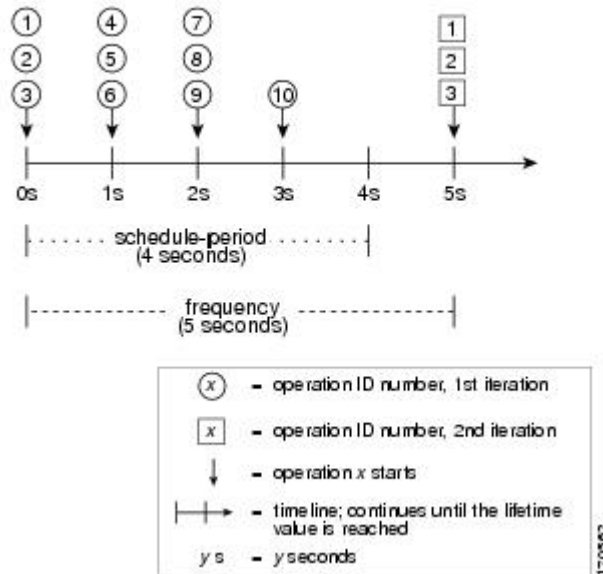
As the frequency is set to 10 in this example, each iteration of operation group 3 will start 10 seconds after the start of the previous iteration. However, this distribution is not optimal as there is a gap of 5 seconds (frequency minus schedule period) between the cycles.

If the number of operations getting scheduled does not equally divide into 1-second intervals, then the operations are equally divided at the start of the schedule period with the remaining operations to start at the last 1-second interval.

The figure below illustrates the scheduling of operation 1 to operation 10 within operation group 4. Operation group 4 has a schedule period of 4 seconds and a frequency of 5 seconds.

Figure 7: 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
```



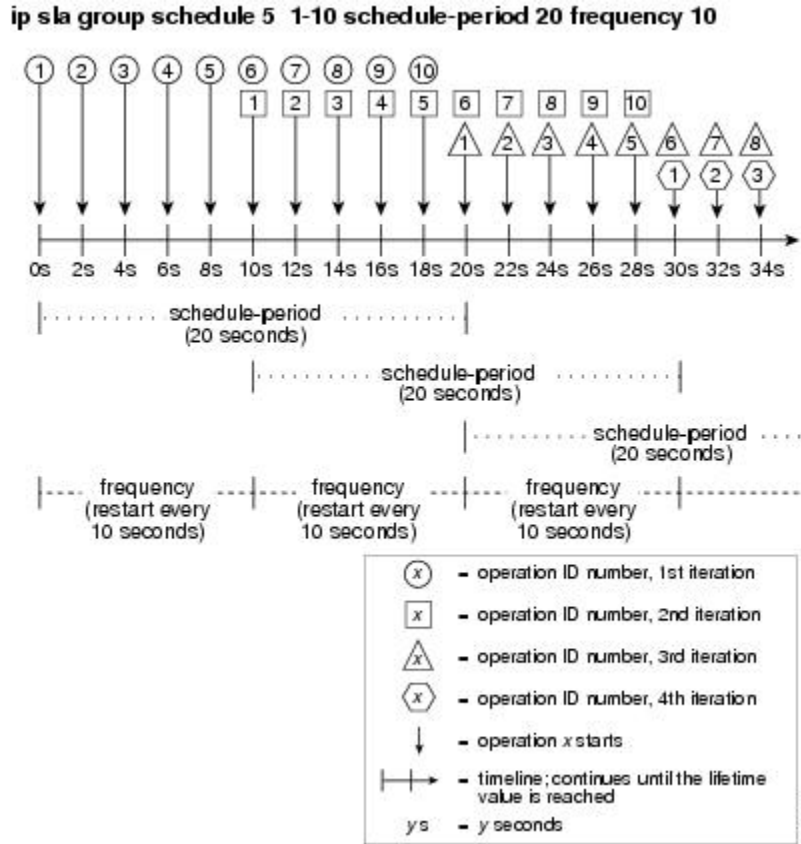
In this example, the IP SLAs multiple operations scheduling functionality calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (10 operations divided by 4 seconds, which equals 2.5 operations every 1 second). Since the number 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 8: IP SLAs Group Scheduling with Schedule Period Greater Than Frequency



In this example, the first operation (operation 1) in operation group 5 will start at 0 seconds. All 10 operations in operation group 5 (operation 1 to operation 10) must be started in the schedule period of 20 seconds. The start time of each IP SLAs operation is evenly distributed over the schedule period by dividing the schedule period by the number of operations (20 seconds divided by 10 operations). Therefore, each operation will start 2 seconds after the previous operation.

In the first iteration of operation group 5, operation 1 starts at 0 seconds, and operation 10, the last operation in the operation group, starts at 18 seconds. Because the operation group is configured to restart every 10 seconds (**frequency 10**), the second iteration of operation group 5 starts again at 10 seconds, before the first iteration is completed. Therefore, an overlap of operations 6 to 10 of the first iteration occurs with operations 1 to 5 of the second iteration during the time period of 10 to 18 seconds (see the figure above). Similarly, there is an overlap of operations 6 to 10 of the second iteration with operations 1 to 5 of the third iteration during the time period of 20 to 28 seconds.

In this example, the start time of operation 1 and operation 6 need not be at exactly the same time, but will be within the same 2-second interval.

The configuration described in this section is not recommended as you can configure multiple operations to start within the same 1-second interval by configuring the number of operations greater than the schedule period. For information, see the "Multiple Operations Scheduling When the Number of IP SLAs Operations Are Greater Than the Schedule Period" section.

IP SLAs Random Scheduler

The IP SLAs Random Scheduler feature is an enhancement to the existing IP SLAs Multioperation Scheduling feature. The IP SLAs Multioperation Scheduling feature provides the capability to easily schedule multiple IP SLAs operations to begin at intervals equally distributed over a specified duration of time and to restart at a specified frequency. With the IP SLAs Random Scheduler feature, you can now schedule multiple IP SLAs operations to begin at random intervals uniformly distributed over a specified duration of time and to restart at uniformly distributed random frequencies within a specified frequency range. Random scheduling improves the statistical metrics for assessing network performance.



Note The IP SLAs Random Scheduler feature is not in compliance with RFC2330 because it does not account for inter-packet randomness.

The IP SLAs random scheduler option is disabled by default. To enable the random scheduler option, you must set a frequency range when configuring a group schedule in global configuration mode. The group of operations restarts at uniformly distributed random frequencies within the specified frequency range. The following guidelines apply for setting the frequency range:

- The starting value of the frequency range should be greater than the timeout values of all the operations in the group operation.
- The starting value of the frequency range should be greater than the schedule period (amount of time for which the group operation is scheduled). This guideline ensures that the same operation does not get scheduled more than once within the schedule period.

The following guidelines apply if the random scheduler option is enabled:

- The individual operations in a group operation will be uniformly distributed to begin at random intervals over the schedule period.
- The group of operations restarts at uniformly distributed random frequencies within the specified frequency range.
- The minimum time interval between the start of each operation in a group operation is 100 milliseconds (0.1 seconds). If the random scheduler option is disabled, the minimum time interval is 1 second.
- Only one operation can be scheduled to begin at any given time. If the random scheduler option is disabled, multiple operations can begin at the same time.
- The first operation will always begin at 0 milliseconds of the schedule period.
- The order in which each operation in a group operation begins is random.

How to Configure an IP SLAs Multioperation Scheduler

Scheduling Multiple IP SLAs Operations



Note

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <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 group schedule <i>group-operation-number operation-id-numbers schedule-period schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life { forever <i>seconds</i> }] [start-time { <i>hh:mm:ss</i> <i>month day</i> <i>day month</i> } pending now after <i>hh:mm:ss</i>] Example: 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. <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 group schedule <i>group-operation-number operation-id-numbers</i> schedule-period <i>seconds</i> [ageout <i>seconds</i>] [frequency [<i>seconds</i> range <i>random-frequency-range</i>]] [life { forever <i>seconds</i> }] [start-time { <i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>]} pending now after <i>hh:mm:ss</i> }]	Specifies the scheduling parameters of a group of IP SLAs operations. <ul style="list-style-type: none"> • To enable the IP SLAs random scheduler option, you must configure the frequency range <i>random-frequency-range</i> keywords and argument.

	Command or Action	Purpose
	Example: Device(config)# ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100	
Step 4	exit Example: Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Verifying IP SLAs Multiple Operations Scheduling

SUMMARY STEPS

1. show ip sla statistics
2. show ip sla group schedule
3. show ip sla configuration

DETAILED STEPS

	Command or Action	Purpose
Step 1	show ip sla statistics Example: Device# show ip sla statistics	(Optional) Displays the IP SLAs operation details.
Step 2	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays the IP SLAs group schedule details.
Step 3	show ip sla configuration Example: Device# show ip sla configuration	(Optional) Displays the IP SLAs configuration details.

Examples

After you have scheduled the multiple IP SLAs operations, you can verify the latest operation details using the appropriate **show** commands.

The following example schedules IP SLAs operations 1 through 20 in the operation group 1 with a schedule period of 60 seconds and a life value of 1200 seconds. By default, the frequency is equivalent to the schedule period. In this example, the start interval is 3 seconds (schedule period divided by number of operations).

```
Device# ip sla group schedule 1 1-20 schedule-period 60 life 1200
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla group schedule** command.

```
Device# show ip sla group schedule
Group Entry Number: 1
Probes to be scheduled: 1-20
Total number of probes: 20
Schedule period: 60
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
```

The following example shows the details of the scheduled multiple IP SLAs operation using the **show ip sla configuration** command. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE).

```
Device# show ip sla configuration 1
Entry number: 1
Owner:
Tag:
Type of operation to perform: udpEcho
Target address: 10.2.31.121
Source address: 0.0.0.0
Target port: 9001
Source port: 0
Request size (ARR data portion): 16
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 1200
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Group Scheduled : TRUE
```

The following example shows the latest operation start time of the scheduled multiple IP SLAs operation, when the operations are scheduled at equal intervals, using the **show ip sla statistics** command:

```
Device# show ip sla statistics | include Latest operation start time
Latest operation start time: *03:06:21.760 UTC Tue Oct 21 2003
Latest operation start time: *03:06:24.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:27.751 UTC Tue Oct 21 2003
```



```

Latest operation start time: *03:06:30.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:33.754 UTC Tue Oct 21 2003
Latest operation start time: *03:06:36.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:39.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:42.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:45.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:48.752 UTC Tue Oct 21 2003
Latest operation start time: *03:06:51.753 UTC Tue Oct 21 2003
Latest operation start time: *03:06:54.755 UTC Tue Oct 21 2003
Latest operation start time: *03:06:57.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:00.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:03.754 UTC Tue Oct 21 2003
Latest operation start time: *03:07:06.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:09.752 UTC Tue Oct 21 2003
Latest operation start time: *03:07:12.753 UTC Tue Oct 21 2003
Latest operation start time: *03:07:15.755 UTC Tue Oct 21 2003
Latest operation start time: *03:07:18.752 UTC Tue Oct 21 2003

```

Configuration Examples for an IP SLAs Multioperation Scheduler

Example Scheduling Multiple IP SLAs Operations

The following example shows how to 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

Related Documents

Related Topic	Document Title
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