IP SLAs Configuration Guide, Cisco IOS XE 17 (Cisco NCS 520)

First Published: 2019-11-26

Last Modified: 2020-01-16

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

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

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

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

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

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

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

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)

© 2020 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

CHAPTER 2 **Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations** 7

- Prerequisites for ITU-T Y.1731 Operations 7
- Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) 7
- How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 8
  - Configuring a Dual-Ended Ethernet Delay or Delay Variation Operation 8
    - Configuring a Receiver MEP on the Destination Device 8
    - Configuring the Sender MEP on the Source Router 10
  - Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation 13
  - Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation 16
  - Scheduling IP SLAs Operations 18
  - Enabling NTP Time of Day Synchronization 20
- Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 21
  - Example: Dual-Ended Ethernet Delay Operation 21
  - Example: Frame Delay and Frame Delay Variation Measurement Configuration 22
  - Example: Sender MEP for a Single-Ended Ethernet Delay Operation 23
  - Example: Sender MEP for a Single-Ended Ethernet Frame Loss Operation 24

Example: Verifying NTP Time Of Day Synchronization 24
Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 25
Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 26

CHAPTER 3 IPSLA Y1731 On-Demand and Concurrent Operations 27
Prerequisites for ITU-T Y.1731 Operations 27
Restrictions for IP SLAs Y.1731 On-Demand Operations 27
Information About IP SLAs Y.1731 On-Demand and Concurrent Operations 28
IPSLA Y1731 SLM Feature Enhancements 28
How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations 29
Configuring a Direct On-Demand Operation on a Sender MEP 29
Configuring a Referenced On-Demand Operation on a Sender MEP 30
Configuring an IP SLAs Y.1731 Concurrent Operation on a Sender MEP 30
Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations 31
Example: On-Demand Operation in Direct Mode 31
Example: On-Demand Operation in Referenced Mode 32
Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations 33
Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations 35

CHAPTER 4 IP SLAs TWAMP Responder 37
Prerequisites for IP SLAs TWAMP Responder 37
Restrictions for IP SLAs TWAMP Responder 37
IP SLAs TWAMP Architecture 38
Two-Way Active Measurement Protocol (TWAMP) 38
TWAMP Protocols 38
IP SLAs TWAMP Responder 39
Configure an IP SLAs TWAMP Responder 40
Configuring the TWAMP Server 40
Configuring the Session Reflector 42
Configuration Example for IP SLAs TWAMP Responder 43

CHAPTER 5 ITU-T Y.1731 Performance Monitoring in a Service Provider Network 45
Prerequisites for ITU-T Y.1731 Performance Monitoring in a Service Provider Network 45
Restrictions for ITU-T Y.1731 Performance Monitoring in a Service Provider Network 45

Information About ITU-T Y.1731 Performance Monitoring in a Service Provider Network **46**
  Frame Delay and Frame-Delay Variation **46**
  Benefits of ITU-T Y.1731 Performance Monitoring **48**
How to Configure ITU-T Y.1731 Performance Monitoring in a Service Provider Network **48**
  Configuring Performance Monitoring Parameters **48**
Configuration Examples for Configuring ITU-T Y.1731 Performance Monitoring Functions **48**
  Example: Configuring Performance Monitoring **48**
Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network **48**

CHAPTER 6 **Configuring an SLM** **51**
Configuring an SLM **51**
  Scheduling an IP SLA Operation **55**

CHAPTER 7 **Configuring DMM over VPLS** **57**
Restrictions for DMM support over VPLS **57**
Configuring DMM over VPLS **57**
Configuration Example for DMM over VPLS **58**
  Configuration Verification Example for DMM over VPLS **59**

CHAPTER 8 **Configuring Loss Measurement Management** **61**
Prerequisites for LMM **61**
Restrictions for Smart SFP **61**
Information About Loss Measurement Management (LMM) **62**
  Y.1731 Performance Monitoring (PM) **62**
    ITU-T Y.1731 Performance Monitoring in a Service Provider Network **63**
    Y.1731 Scalability of **63**
  Frame Delay and Frame-Delay Variation **63**
  Overview of Smart SFP **64**
  Connectivity **65**
  IP SLA **65**
Configuring Loss Measurement Management **65**
  Configuring LMM **65**
  Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation **68**
Configuration Examples for LMM **70**

Verifying LMM 71
Additional References 72
Feature Information for Loss Measurement Management (LMM) with Smart SFP 73

CHAPTER 9 IP SLA—Service Performance Testing 75
Finding Feature Information 75
Information About Service Performance Operations 75
Information About Configuring Y.1564 to Generate and Measure Ethernet Traffic 77
Prerequisites for IP SLA - Service Performance Testing 78
Scale and Limitations for Configuring IP SLA - Service Performance Operation 78
Restrictions for IP SLA - Service Performance Operation 79
Generating Traffic Using Y.1564 81
How to Configure IP SLA - Service Performance Testing 83
  Configuring Ethernet Target Two-Way Color Blind Session 83
Configuration Examples for Configuring Y.1564 to Generate and Measure Ethernet Traffic 86
  Example: Traffic Generation 86
  Example: Two-Way Session 87
  Example: Passive Measurement Mode 87
  Example: Two-Way Measurement Mode 88
Additional References for IP SLA - Service Performance Testing 89

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

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 .

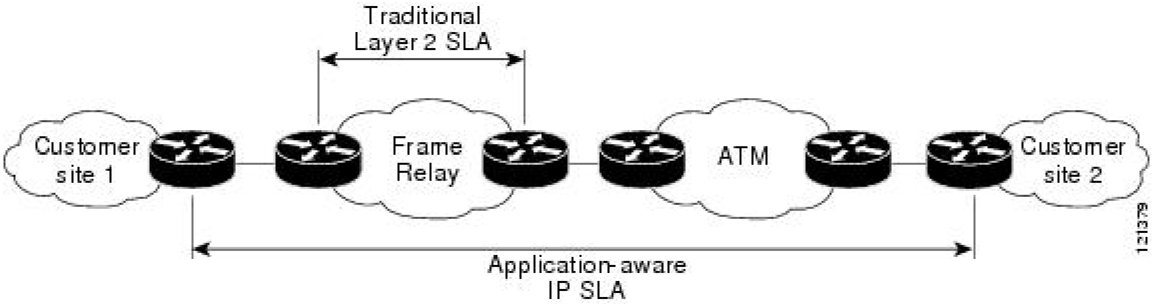
SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and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

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 .

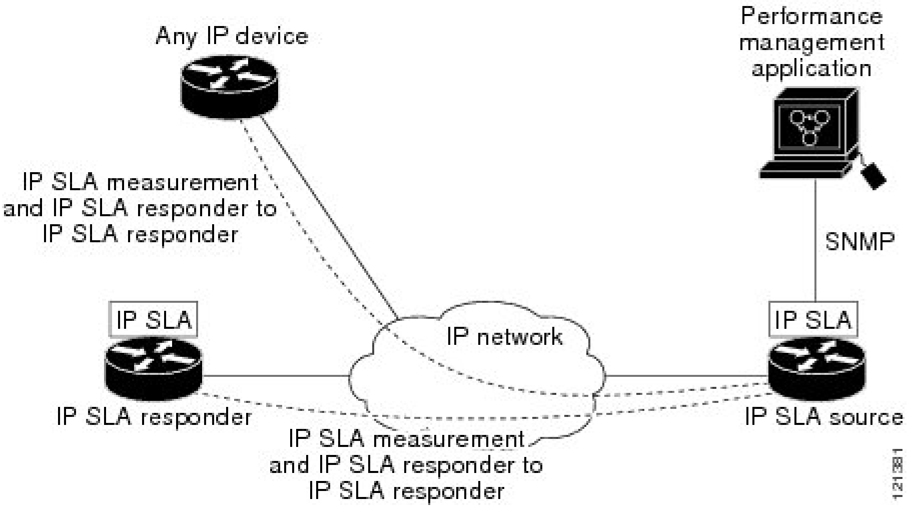
Network Performance Measurement Using IP SLAs

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


Any IP device
Performance management application
IP SLA measurement and IP SLA responder to IP SLA responder
SNMP
IP SLA
IP network
IP SLA
IP SLA responder
IP SLA source
IP SLA measurement and IP SLA responder to IP SLA responder
121381

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.

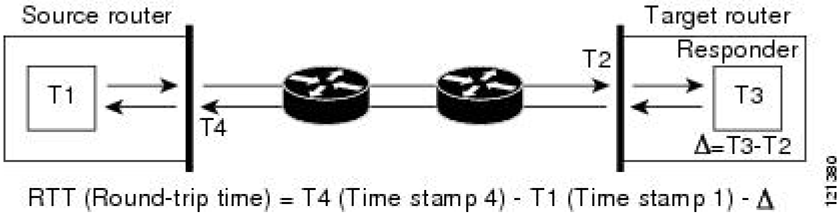
Response Time Computation for IP SLAs

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


Source router
Target router
Responder
T1
T2
T3
T4
Δ=T3-T2
RTT (Round-trip time) = T4 (Time stamp 4) - T1 (Time stamp 1) - Δ
121380

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.

CHAPTER 2

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 7
- Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731), on page 7
- How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations, on page 8
- Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations, on page 21
- Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations , on page 25
- Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations, on page 26

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)

- Depending on your Cisco software release, SNMP is not supported for reporting threshold events or collecting performance statistics for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operations.
- 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.
- P2 IMs are to be used for CFM and Y1731.
- Do not configure rewrite on the EFPs throughout the l2 circuit to avoid losing the cos value.
- To avoid errors in RX and TX timestamping, ensure to have Y1731 sender as PTP master, and the Y1731 responder as PTP slave.
- Reconfigure IP SLA Y1731 while doing online insertion removal (OIR) of IM or router reload because local MEP is deleted during the course.
- 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config-term)# ip sla 501`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 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*} **Example:** `Router(config-ip-sla)# ethernet y1731 delay receive 1DM domain xxx evc yyy cos 3 mpid 101`	Begins configuring the receiver on the responder and enters IP SLA Y.1731 delay configuration mode. • The *source-mp-id* or *source-address* configured by this command corresponds to that of the MEP being configured. **Note** The session with mac-address will not be inactivated when there is CFM error.
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-delay)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 6	**distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,...,***boundary*] **Example:** `Router(config-sla-y1731-delay)# distribution delay-variation one-way 5`	(Optional) Specifies measurement type and configures bins for statistics distributions kept.

	Command or Action	Purpose
	`5000,10000,15000,20000,-1`	
Step 7	**frame offset** *offset-value* **Example:** `Router(config-sla-y1731-delay)# frame offset 1`	(Optional) Sets the value for calculating delay variation rates.
Step 8	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-delay)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 9	**max-delay** *milliseconds* **Example:** `Router(config-sla-y1731-delay)# max-delay 5000`	(Optional) Sets the amount of time an MEP waits for a frame.
Step 10	**owner** *owner-id* **Example:** `Router(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation.
Step 11	**end** **Example:** `Router(config-sla-y1731-delay)# end`	Exits to privileged EXEC mode.

What to do next

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

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

Configuring 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 proacive 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:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla operation-number** **Example:** `Router(config)# ip sla 500`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 delay 1DM domain domain-name** {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} **Example:** `Router(config-ip-sla)# ethernet y1731 delay 1DM domain xxx evc yyy mpid 101 cos 3 source mpid 100`	Begins configuring a dual-ended Ethernet delay operation and enters IP SLA Y.1731 delay configuration mode. **Note** The session with mac-address will not be inactivated when there is CFM error.

	Command or Action	Purpose
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-delay)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 6	**frame interval** *milliseconds* **Example:** `Router(config-sla-y1731-delay)# frame interval 100`	(Optional) Sets the gap between successive frames.
Step 7	**frame size** *bytes* **Example:** `Router(config-sla-y1731-delay)# frame size 64`	(Optional) Sets the padding size for frames.
Step 8	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-delay)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 9	**owner** *owner-id* **Example:** `Router(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation.
Step 10	**end** **Example:** `Router(config-sla-y1731-delay)# end`	Exits to privileged EXEC mode.

What to do next

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

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

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

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

Before you begin

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

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

SUMMARY STEPS

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

	Command or Action	Purpose
Step 3	**ip sla** *operation-number* **Example:** `Device(config-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. • 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. **Note** The session with mac-address will not be inactivated when there is CFM error.
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:** `Device(config-sla-y1731-delay)# frame interval 100`	(Optional) Sets the gap between successive frames.

	Command or Action	Purpose
Step 9	**frame offset** *offset-value* **Example:** `Device(config-sla-y1731-delay)# frame offset 1`	(Optional) Sets value for calculating delay variation values.
Step 10	**frame size** *bytes* **Example:** `Device(config-sla-y1731-delay)# frame size 32`	(Optional) Configures padding size for frames.
Step 11	**history interval** *intervals-stored* **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** *milliseconds* **Example:** `Device(config-sla-y1731-delay)# max-delay 5000`	(Optional) Sets the amount of time an MEP waits for a frame.
Step 13	**owner** *owner-id* **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 To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

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

Before you begin

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Device(config-term)# ip sla 11`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 loss** {**LMM** | **SLM**} [**burst**] **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **CoS** *CoS* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} **Example:** `Device(config-ip-sla)# ethernet y1731 loss LMM domain xxx vlan 12 mpid 34 CoS 4 source mpid 23`	Begins configuring a single-ended Ethernet frame loss ratio operation and enters IP SLA Y.1731 loss configuration mode. • 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. **Note** The session with mac-address will not be inactivated when there is CFM error.
Step 5	**aggregate interval** *seconds* **Example:** `Device(config-sla-y1731-loss)# aggregate interval 900`	(Optional) Configures the length of time during which performance measurements are conducted and the results stored.
Step 6	**availability algorithm** {**sliding-window** | **static-window**} **Example:** `Device(config-sla-y1731-loss)# availability algorithm static-window`	(Optional) Specifies availability algorithm used.
Step 7	**frame consecutive** *value* **Example:** `Device(config-sla-y1731-loss)# frame consecutive 10`	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status.

	Command or Action	Purpose
Step 8	**frame interval** *milliseconds* **Example:** `Device(config-sla-y1731-loss)# frame interval 100`	(Optional) Sets the gap between successive frames.
Step 9	**history interval** *intervals-stored* **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** *owner-id* **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	**exit** **Example:** `Device(config)# exit`	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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] • **ip sla group schedule** *group-operation-number operation-id-numbers* {**schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}] **Example:** `Device(config)# ip sla schedule 10 life forever start-time now`	• Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

	Command or Action	Purpose

	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

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

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. **platfrom time-source ntp**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platfrom 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
      TX Time BWD                  RX Time BWD               Frame Delay
      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
Ethernet CFM	“Configuring Ethernet Connectivity Fault Management in a Service Provider Network” module of the *Cisco IOS Carrier Ethernet Configuration Guide*
Network Time Protocol (NTP)	“Configuring NTP” module of the *Cisco IOS Network Management Configuration Guide*
Proactive threshold monitoring for Cisco IOS IP SLAs	“Configuring Proactive Threshold Monitoring of IP SLAs Operations” module of the *Cisco IOS IP SLAs Configuration Guide*

Standards and RFCs

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

MIBs

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

Technical Assistance

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

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

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

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

Table 1: Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Feature Name	Releases	Feature Information
IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).

CHAPTER 3

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 27
- Restrictions for IP SLAs Y.1731 On-Demand Operations, on page 27
- Information About IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 28
- How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 29
- Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 31
- Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 33
- Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 35

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. • Enter your password if prompted.
Step 2	**ip sla on-demand ethernet** {**DMMv1** | **SLM**} **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} {**continuous** [**interval** *milliseconds*] | **burst** [**interval** *milliseconds*] [**number** *number-of-frames*] [**frequency** *seconds*]} [**size** *bytes*] **aggregation** *seconds* {**duration** *seconds* | **max** *number-of-packets*} **Example:**	Creates and runs an on-demand operation in direct mode. • 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. • 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. • 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
```

```
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 *Carrier Ethernet Configuration Guide*
Ethernet operations	“Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations” module of the *IP SLAs Configuration Guide*
Network Time Protocol (NTP)	“Configuring NTP” module of the *Network Management Configuration Guide*

Standards and RFCs

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

MIBs

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

Technical Assistance

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

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

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

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

Table 2: Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations

Feature Name	Releases	Feature Information
IP SLAs Y.1731 On-Demand and Concurrent Operations	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).

CHAPTER 4

IP SLAs TWAMP Responder

The Two-Way Active Measurement Protocol (TWAMP) defines a flexible method for measuring round-trip IP performance between any two devices.

TWAMP enables complete IP performance measurement. TWAMP also provides a flexible choice of solutions because it supports all devices deployed in the network.

This chapter describes how to configure the Two-Way Active Measurement Protocol (TWAMP) responder on a Cisco device to measure IP performance between the Cisco device and a non-Cisco TWAMP control device on your network.

Note IPv6 is supported for IP SLA TWAMP Responder on the RSP3 module.

- Prerequisites for IP SLAs TWAMP Responder, on page 37
- Restrictions for IP SLAs TWAMP Responder, on page 37
- IP SLAs TWAMP Architecture, on page 38
- Configure an IP SLAs TWAMP Responder, on page 40
- Configuration Example for IP SLAs TWAMP Responder, on page 43

Prerequisites for IP SLAs TWAMP Responder

- A TWAMP control client and a session sender must be configured in your network.
- IP SLA responder must be configured on the device. Use the command **ip sla responder twamp** to configure IP SLA responder.
- Enable NTP time stamping for TWAMP test packet.
- Enable PTP time stamping for TWAMP test packet.

Restrictions for IP SLAs TWAMP Responder

- Time stamping is not supported for TWAMP test packets that ingress or egress through management interfaces. Time stamping is supported only on BDI interfaces.

- TWAMP client and session sender are not supported.
- TWAMP Light mode is not supported until the Cisco IOS XE Bengaluru 17.4.1 release.

IP SLAs TWAMP Architecture

Two-Way Active Measurement Protocol (TWAMP)

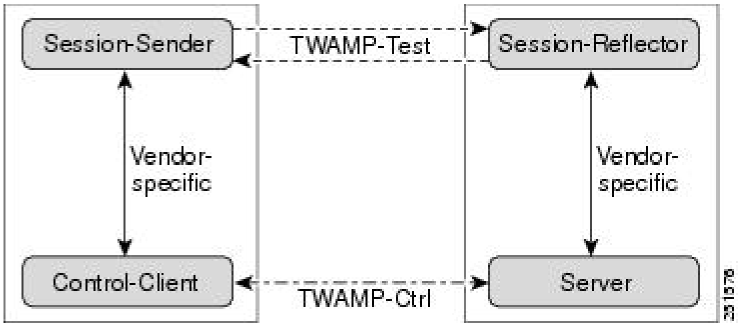
The IETF Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the TWAMP protocols. The TWAMP-Control protocol is used to set up performance measurement sessions. The TWAMP-Test protocol is used to send and receive performance measurement probes.

The TWAMP architecture is composed of the following four logical entities that are responsible for starting a monitoring session and exchanging packets:

- The control client: It sets up, starts, and stops TWAMP test sessions.
- The session sender: It instantiates TWAMP test packets that are sent to the session reflector.
- The session reflector: It reflects a measurement packet upon receiving a TWAMP test packet. The session reflector does not collect packet statistics in TWAMP.
- The TWAMP server: It is an end system that manages one or more TWAMP sessions and is also capable of configuring each session ports in the end points. The server listens on the TCP port. The session-reflector and server make up the TWAMP responder in an IP SLAs operation.

Although TWAMP defines the different entities for flexibility, it also allows for logical merging of the roles on a single device for ease of implementation. The figure below shows the interactions of four entities of the TWAMP architecture.

Figure 4: TWAMP Architecture



TWAMP Protocols

The TWAMP protocol includes three distinct message exchange categories, they are:

- Connection setup exchange—Messages establish a session connection between the control client and the server. First, the identities of the communicating peers are established via a challenge response mechanism. The server sends a randomly generated challenge, to which the control client then sends a response by encrypting the challenge using a key derived from the shared secret. Once the identities are established, the next step negotiates a security mode that is binding for the subsequent TWAMP-Control commands as well as the TWAMP-Test stream packets.

Note A server can accept connection requests from multiple control clients.

- TWAMP control exchange—The TWAMP control protocol runs over TCP and is used to instantiate and control measurement sessions. The sequence of commands is as follows:
  - request session
  - start session
  - stop session

  However, unlike the connection setup exchanges, the TWAMP control commands can be sent multiple times. However, the messages cannot occur out of sequence although multiple request session commands can be sent before a session start command.

- TWAMP test stream exchange—The TWAMP test runs over UDP and exchanges TWAMP test packets between session sender and session reflector. These packets include timestamp fields that contain the instant of packet egress and ingress. The packet also includes a sequence number.

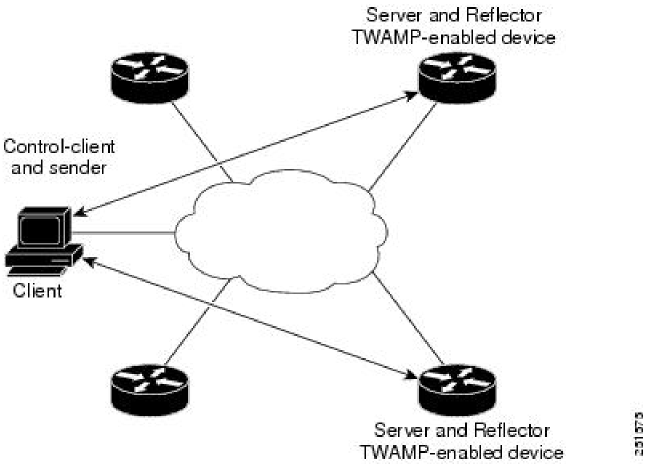
Note TWAMP control and TWAMP test stream support only unauthenticated security mode.

IP SLAs TWAMP Responder

A TWAMP responder interoperates with the control client and session sender on another device that supports TWAMP. In the current implementation, the session reflector and TWAMP server that make up the responder must be co-located on the same device.

In the figure below, one device is the control client and session-sender (TWAMP control device), and the other two devices are Cisco devices that are configured as IP SLAs TWAMP responders. Each IP SLAs TWAMP responder is both a TWAMP server and a session-reflector.

Figure 5: IP SLAs TWAMP Responders in a Basic TWAMP Deployment


Server and Reflector
TWAMP-enabled device
Control-client
and sender
Client
Server and Reflector
TWAMP-enabled device
251575

Note NCS 520supports only hardware time stamping.

Configure an IP SLAs TWAMP Responder

Note Effective Cisco IOS-XE Everest 16.6.1, time stamping for sender (T1, T4) and receiver (T3, T2) is performed by the hardware, instead of the software. This time stamping is done bythe hardware to improve the accuracy of jitter and latency measurements.

Note Software time stamping is implemented for TWAMP IP SLA packets on the RSP3 module.

Configuring the TWAMP Server

Note In the current implementation of IP SLAs TWAMP Responder, the TWAMP server and the session reflector must be configured on the same device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla server twamp**
4. **port** *port-number*

5. **timer inactivity** *seconds*
6. **end**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ip sla server twamp**

Example:

```
Device(config)#  ip sla server twamp
```

Configures the device as a TWAMP server and enters TWAMP server configuration mode.

Step 4 **port** *port-number*

Example:

```
Device(config-twamp-srvr)# port 9000
```

(Optional) Configures the port to be used by the TWAMP server to listen for connection and control requests.

Step 5 **timer inactivity** *seconds*

Example:

```
Device(config-twamp-srvr)# timer inactivity 300
```

(Optional) Configures the inactivity timer for a TWAMP control session.

Step 6 **end**

Example:

```
Device(config-twamp-srvr)# end
```

Returns to privileged EXEC mode.

Configuring the Session Reflector

Note In the current implementation of IP SLAs TWAMP Responder, the TWAMP server and the session reflector must be configured on the same device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder twamp**
4. **timeout** *seconds*
5. **end**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ip sla responder twamp**

Example:

```
Device(config)# ip sla responder twamp
```

Configures the device as a TWAMP responder and enters TWAMP reflector configuration mode.

Step 4 **timeout** *seconds*

Example:

```
Device(config-twamp-ref)#  timeout 300
```

(Optional) Configures an inactivity timer for a TWAMP test session.

Step 5 **end**

Example:

```
Device(config-twamp-ref)# end
```

Exits to privileged EXEC mode.

Configuration Example for IP SLAs TWAMP Responder

The following example and partial output shows how to configure the TWAMP server and the session reflector on the same Cisco device. In this configuration, port 862 is the (default) port to be used by the TWAMP server to listen for connection and control requests. The port for the server listener is the RFC-specified port and if required, can be reconfigured.

Note For the IP SLAs TWAMP responder to function, a control client and the session sender must be configured in your network.

The following examples are for non-VRF scenarios (default):

```
Device> enable
Device# configure terminal
Router(config)# ip sla serv twamp
Router(config-twamp-srvr)# port 12000
Router(config-twamp-srvr)# timer inactivity 1200
Router(config-twamp-srvr)# exit
Router(config)# ip sla responder tw
Router(config)# ip sla responder twamp
Router(config-twamp-ref)# resp
Router(config-twamp-ref)# time
Router(config-twamp-ref)# timeout 2000
Router(config-twamp-ref)# exit

Router# show ip sla twamp connection requests
    Connection-Id     Client Address   Client Port      Client VRF
          A3              100.1.0.1         59807         default

Router# show ip sla twamp connection detail
Connection Id:          A3
  Client IP Address:    100.1.0.1
  Client Port:          59807
  Client VRF:           intf2
  Mode:                 Unauthenticated
  Connection State:     Connected
  Control State:        Active
  Number of Test Requests - 0:1

Router# show ip sla twamp session
IP SLAs Responder TWAMP is: Enabled
Recvr Addr: 100.1.0.2
Recvr Port: 7
Sender Addr: 100.1.0.1
Sender Port: 34608
Sender VRF: default
Session Id: 100.1.0.2:15833604877498391199:6D496912
Connection Id: 101

Router# sh running-config | b twamp
ip sla responder twamp
```

```
 timeout 2000
ip sla responder
ip sla enable reaction-alerts
ip sla server twamp
 port 12000
 timer inactivity 1200
!
!
```

The following examples are for VRF scenarios:

```
Router# show ip sla twamp session
IP SLAs Responder TWAMP is: Enabled
Recvr Addr: 100.1.0.2
Recvr Port: 7
Sender Addr: 100.1.0.1
Sender Port: 51486
Sender VRF: intf1
Session Id: 100.1.0.2:9487538053959619969:73D5EDEA
Connection Id: D0

Router# show ip sla twamp connection detail
Connection Id:          A3
  Client IP Address:    100.1.0.1
  Client Port:          52249
  Client VRF:           intf2
  Mode:                 Unauthenticated
  Connection State:     Connected
  Control State:        Active
  Number of Test Requests - 0:1

Router# show ip sla twamp connection requests
  Connection-Id    Client Address   Client Port    Client VRF
             A3       100.1.0.1       52249          intf2
 Total number of current connections: 1
```

Note The default port for IP SLA server is 862.

CHAPTER 5

ITU-T Y.1731 Performance Monitoring in a Service Provider Network

ITU-T Y.1731 performance monitoring provides standard-based Ethernet performance monitoring that encompasses the measurement of Ethernet frame delay, frame-delay variation, and throughput as outlined in the ITU-T Y.1731 specification and interpreted by the Metro Ethernet Forum (MEF). Service providers offer service level agreements (SLAs) that describe the level of performance customers can expect for services. This document describes the Ethernet performance management aspect of SLAs.

- Prerequisites for ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 45
- Restrictions for ITU-T Y.1731 Performance Monitoring in a Service Provider Network , on page 45
- Information About ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 46
- How to Configure ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 48
- Configuration Examples for Configuring ITU-T Y.1731 Performance Monitoring Functions, on page 48
- Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 48

Prerequisites for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

- For Y.1731 performance monitoring to work, connectivity fault management (CFM) sessions should be up and running.
- Continuity check messages (CCM) database should be populated.

Restrictions for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

- The frame-delay measurement message (DMM) with CFM over cross-connect on the router works only if the **control-word** command is enabled.

- When the core network has multiple paths, the Tx and Rx, DMM/DMR packets can be sent and received on different ports. If the ports belong to a different interface module (IM), time stamping can be out of sync and in certain cases the Rx value can be lower than the Tx value. This value is displayed as 0 in the raw database output. As a workaround, configure Precision Time Protocol (PTP) between the two connectivity fault management (CFM) endpoint routers.
- Y.1731 is supported with the **rewrite**command configuration on Ethernet Flow Points (EFPs) throughout the Layer 2 circuit. However, the configuration may be in such a way that the Y1731 PDUs may be transmitted untagged. This results in the other end of the Layer 2 circuit not being able to ascertain the CoS value which determines the SLA session to which the PDUs belong. Therefore, the **rewrite** command configuration is *not* supported when CoS value is configured with IP SLA or the Y.1731 profile.
- Y.1731 performance monitoring is *not* supported in MEPs that are configured on ports.
- Y.1731 DMM is not supported on the RSP3 platform, when there are two VLAN tags, two or more MPLS tag with control word enabled on the system.

Note In ITU-T Y1731, 1DM measurement should mandate only PTP to have clock sync between sender & receiver.

Information About ITU-T Y.1731 Performance Monitoring in a Service Provider Network

Frame Delay and Frame-Delay Variation

The Frame Delay parameter can be used for on-demand OAM measurements of frame delay and frame-delay variation. When a maintenance end point (MEP) is enabled to generate frames with frame-delay measurement (ETH-DM) information, it periodically sends frames with ETH-DM information to its peer MEP in the same maintenance entity. Peer MEPs perform frame-delay and frame-delay variation measurements through this periodic exchange during the diagnostic interval.

An MEP requires the following specific configuration information to support ETH-DM:

- MEG level—MEG level at which the MEP exists
- Priority
- Transmission rate
- Total interval of ETH-DM

A MEP transmits frames with ETH-DM information using the TxTimeStampf information element. TxTimeStampf is the time stamp for when the ETH-DM frame was sent. A receiving MEP can compare the TxTimeStampf value with the RxTimef value, which is the time the ETH-DM frame was received, and calculate one-way delay using the formula *frame delay = RxTimef – TxTimeStampf*.

One-way frame-delay measurement (1DM) requires that clocks at both the transmitting MEP and the receiving MEPs are synchronized. Measuring frame-delay variation does not require clock synchronization and the variation can be measured using 1DM or a frame-delay measurement message (DMM) and a frame-delay measurement reply (DMR) frame combination.

If it is not practical to have clocks synchronized, only two-way frame-delay measurements can be made. In this case, the MEP transmits a frame containing ETH-DM request information and the TxTimeStampf element, and the receiving MEP responds with a frame containing ETH-DM reply information and the TxTimeStampf value copied from the ETH-DM request information.

Two-way frame delay is calculated as *(RxTimeb–TxTimeStampf)–(TxTimeStampb–RxTimeStampf)*, where RxTimeb is the time that the frame with ETH-DM reply information was received. Two-way frame delay and variation can be measured using only DMM and DMR frames.

To allow more precise two-way frame-delay measurement, the MEP replying to a frame with ETH-DM request information can also include two additional time stamps in the ETH-DM reply information:

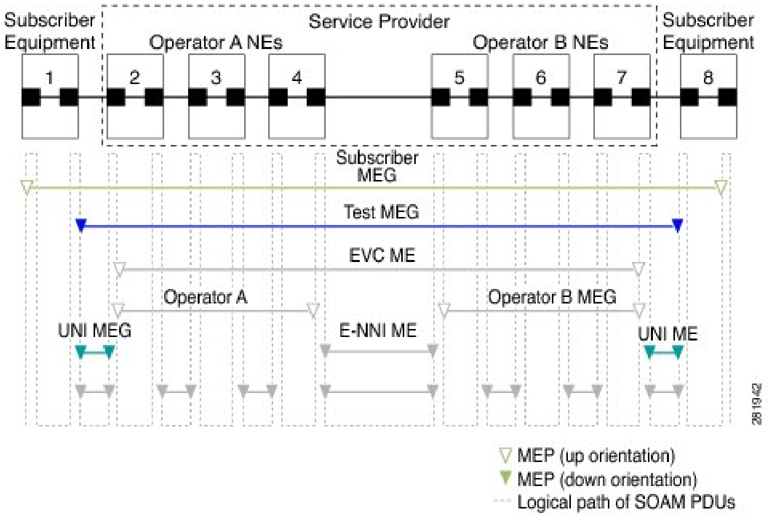
- RxTimeStampf—Time stamp of the time at which the frame with ETH-DM request information was received.
- TxTimeStampb—Time stamp of the time at which the transmitting frame with ETH-DM reply information was sent.
- The timestamping happens at the hardware level for DMM operations.

Note The frame-loss, frame-delay, and frame-delay variation measurement processes are terminated when faults related to continuity and availability occur or when known network topology changes occur.

An MIP is transparent to the frames with ETH-DM information; therefore, an MIP does not require information to support the ETH-DM function.

The figure below shows a functional overview of a typical network in which Y.1731 performance monitoring is used.

Figure 6: Y.1731 Performance Monitoring


Subscriber Equipment
Service Provider
Operator A NEs
Operator B NEs
Subscriber Equipment
1
2
3
4
5
6
7
8
Subscriber MEG
Test MEG
EVC ME
Operator A
Operator B MEG
UNI MEG
E-NNI ME
UNI ME
281942
MEP (up orientation)
MEP (down orientation)
Logical path of SOAM PDUs

Benefits of ITU-T Y.1731 Performance Monitoring

Combined with IEEE-compliant connectivity fault management (CFM), Y.1731 performance monitoring provides a comprehensive fault management and performance monitoring solution for service providers. This comprehensive solution in turn lessens service providers' operating expenses, improves their service-level agreements (SLAs), and simplifies their operations.

How to Configure ITU-T Y.1731 Performance Monitoring in a Service Provider Network

Configuring Performance Monitoring Parameters

The following new commands were introduced that can be used to configure and display performance monitoring parameters: **debug ethernet cfm pm**, **monitor loss counters**, and **show ethernet cfm pm**.

For more information about CFM and Y.1731 performance monitoring commands, see the *Cisco IOS Carrier Ethernet Command Reference*. For more information about debug commands, see the *Cisco IOS Debug Command Reference*.

Configuration Examples for Configuring ITU-T Y.1731 Performance Monitoring Functions

Example: Configuring Performance Monitoring

For Y.1731 performance monitoring configuration examples, see *Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations*. For information about Y.1731 On-Demand and Concurrent Operations, see *Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations*.

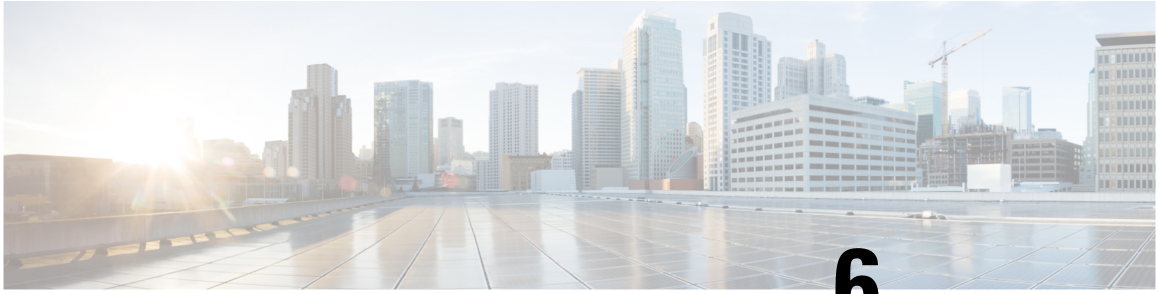
Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

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

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

Table 3: Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

Feature Name	Releases	Feature Information
ITU-T Y.1731 Performance Monitoring in a Service Provider Network	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).



CHAPTER 6

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 an SLM, on page 51

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. **exit**
12. **ip sla reaction-configuration** *operation-number* [**react** {**unavailableDS** |**unavailableSD** | **loss-ratioDS** | **loss-ratioSD**}] [**threshold-type** {**average** [*number -of-measurements*] | **consecutive** [*occurences*] | **immediate**}] [**threshold-value** *upper -threshold lower-threshold*]
13. **ip sla logging traps**
14. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router > enable`	• Enter your password if prompted.
Step 2	**configure terminal** *operation number* **Example:** `Device# configure terminal`	—Identifies the IP SLAs' operation you want to configure. Enters global configuration mode.
Step 3	**ip sla** *operation number* **Example:** `Router(config)# ip sla 11`	Configures an IP SLA operation and enters IP SLA configuration mode. • *operation-number*—Identifies the IP SLAs' operation you want to configure.
Step 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*}} **Example:** `Router(config-ip-sla)# ethernet y1731 loss SLM domain xxx evc yyy mpid 101 cos 4 source mpid 100`	Configures a single-ended synthetic loss measurement and enters IP SLA Y.1731 loss configuration mode. • **EVC**—Specifies the ethernet virtual circuit name. • **SLM**—Specifies that the frames sent are Synthetic Loss Measurement (SLM) frames. • **domain** *domain-name*—Specifies the name of the Ethernet Connectivity Fault Management (CFM) maintenance domain. • **vlan** *vlan-id*—Specifies the VLAN identification number. The range is from 1 to 4094. • **mpid** *target-mp-id*—Specifies the maintenance endpoint identification numbers of the MEP at the destination. The range is from 1 to 8191. • **mac-address** *target-address*—Specifies the MAC address of the MEP at the destination. • **cos** *cos*—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** *source-mp-id*—Specifies the maintenance endpoint identification numbers of the MEP being configured. The range is from 1 to 8191. • **mac-address** *source-address*—Specifies the MAC address of the MEP being configured.

	Command or Action	Purpose
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-loss)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored. - *seconds*—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 1**} **symmetric** **Example:** `Router(config-sla-y1731-loss)# availability algorithm static-window`	(Optional) Specifies availability algorithm used. - **sliding-window**—Specifies a sliding-window control algorithm. - **static-window**—Specifies static-window control algorithm.
Step 7	**frame consecutive** *value* **Example:** `Router(config-sla-y1731-loss)# frame consecutive 10.`	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status. - *value*—Specifies the number of consecutive measurements. The range is from 1 to 10. The default is 10.
Step 8	**frame interval** *milliseconds* **Example:** `Router(config-sla-y1731-loss)# frame interval 1000`	(Optional) Sets the gap between successive frames. - *milliseconds*—Specifies the length of time in milliseconds (ms) between successive synthetic frames. The default is 1000
Step 9	**frame size** *bytes* **Example:** `Router(config-sla-y1731-loss)# frame size 64`	(Optional) Configures padding size for frames. - *bytes*—Specifies the padding size, in four-octet increments, for the synthetic frames. The default is 64.
Step 10	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-loss)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation. - *intervals-stored*—Specifies the number of statistics distributions. The range is from 1 to 10. The default is 2.
Step 11	**exit** **Example:** `Router(config-sla-y1731-loss)# exit`	Exits IP SLA Y.1731 loss configuration mode and enters IP SLA configuration mode.
Step 12	**ip sla reaction-configuration** *operation-number* [**react** {**unavailableDS** |**unavailableSD** | **loss-ratioDS** | **loss-ratioSD**}] [**threshold-type** {**average** [*number -of-measurements*] | **consecutive** [*occurences*] |	(Optional) Configures proactive threshold monitoring for frame loss measurements. - *operation-number*—Identifies the IP SLAs operation for which reactions are to be configured.

	Command or Action	Purpose
	immediate}] [**threshold-value** *upper -threshold lower-threshold*] **Example:** `Router(config)# ip sla reaction-configuration 11 react unavailableDS`	- **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**[*number-of-measurements*]—(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**[*occurrences*] —(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***upper-threshold lower-threshold*—(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements.
Step 13	**ip sla logging traps** **Example:**	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.

	Command or Action	Purpose
	`Router(config)# ip sla logging traps`	
Step 14	**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** *operation-number* [**life** { **forever** | *seconds* }] [**start-time** {*hh* **:** *mm* [**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss* | **random** *milliseconds*}] **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. • *operation-number*—Identifies the IP SLAs operation for which reactions are to be configured. • **life forever**— (Optional) Schedules the operation to run indefinitely. • **life** *seconds* —(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).

	Command or Action	Purpose
		• **start-time** —(Optional) Time when the operation starts. • *hh***:***mm*[**:***ss*]—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. • *month* —(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. • *day* —(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** *hh***:***mm***:***ss*—(Optional) Indicates that the operation should start hh hours, mm minutes, and ss seconds after this command was entered. • **random** *milliseconds*—(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	**exit** **Example:** `Router(config)# exit`	Exits the global configuration mode and enters the privileged EXEC mode.

CHAPTER 7

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 57
- Configuring DMM over VPLS, on page 57
- Configuration Example for DMM over VPLS, on page 58

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 8

Configuring Loss Measurement Management

Loss Measurement Management (LMM) is a loss monitoring feature implemented using the Smart SFP. The LMM functionality is developed to monitor the loss and delay traffic measurement data on the router.

- Prerequisites for LMM, on page 61
- Restrictions for Smart SFP, on page 61
- Information About Loss Measurement Management (LMM), on page 62
- Configuring Loss Measurement Management, on page 65
- Configuration Examples for LMM, on page 70
- Verifying LMM, on page 71
- Additional References, on page 72
- Feature Information for Loss Measurement Management (LMM) with Smart SFP, on page 73

Prerequisites for LMM

- Smart SFP must be installed on the port where Frame Loss Ratio and Availability (Loss Measurements with LMM or LMR) is calculated.
- Continuity check messages (CCM)s must be enabled for LM and DM on the Smart SFP.
- An untagged EFP BD should be configured on the Smart SFP interface for LMM.

Note Smart SFP must be installed on the router running with Cisco IOS XE Release 3.12S and later post the ISSU upgrade. However, if the smart SFP must be installed on a router running prior to Cisco IOS XE Release 3.12S, we recommend that an IM OIR is performed post ISSU upgrade and an SSO performed post ISSU upgrade.

Restrictions for Smart SFP

- Smart SFP does *not* support Digital Optical Monitoring (DOM).
- Maximum number of MEPS supported on the interfaces with Smart SFP is 64.

- Maximum of 2 MEPs can be configured under EFP on a Smart SFP for LMM or Delay measurement management (DMM).
- Off-loaded CC interval is not supported for EVC BD UP MEP.
- Performance management (PM) sessions are generated with an interval of 1 second. The maximum number of sessions that are supported are 1000.
- LMM is *not* supported on the ten gigabit ethernet interface.
- A single Smart SFP can act as an UP or down MEP only.
- A MEP can participate in per cos LM or aggregate LM, but participating on both is *not* supported.
- Y.1731 measurements are *not* supported on the Smart SFP which is connected to a port-channel.
- The UP MEP, CFM and Y.1731 messages initiating or terminating at the MEP, are *not* accounted for in the LM statistics.
- LMM is *not* support on below encapsulations:
    - Untagged
    - Priority-tagged
    - Default tagged
- In the case of EVC BD UP MEP, all the interfaces on the BD participating in performance measurement should have Smart SFPs installed, however the core facing interface associated with the MEP may have a standard SFP installed.
- An untagged EVC BD must be configured on the interface installed with Smart SFP where MEP is configured for LM session.
- Interoperability with platforms supporting long pipe QoS model requires explicit qos policy for cos to exp mapping and vice versa.

Information About Loss Measurement Management (LMM)

Loss measurement management is achieved by using the Smart SFP.

Y.1731 Performance Monitoring (PM)

Y.1731 Performance Monitoring (PM) provides a standard Ethernet PM function that includes measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group. As per recommendations, devices should be able to send, receive and process PM frames in intervals of 1000ms (1000 frames per second) with the maximum recommended transmission period being 1000ms (1000 frames per second) for any given service.

To measure Service Level Agreements (SLAs) parameters, such as frame delay or frame delay variation, a small number of synthetic frames are transmitted along with the service to the end point of the maintenance region, where the Maintenance End Point (MEP) responds to the synthetic frame. For a function such as connectivity fault management, the messages are sent less frequently, while performance monitoring frames are sent more frequently.

ITU-T Y.1731 Performance Monitoring in a Service Provider Network

ITU-T Y.1731 performance monitoring provides standard-based Ethernet performance monitoring that encompasses the measurement of Ethernet frame delay, frame-delay variation, and throughput as outlined in the ITU-T Y.1731 specification and interpreted by the Metro Ethernet Forum (MEF). Service providers offer service level agreements (SLAs) that describe the level of performance customers can expect for services. This document describes the Ethernet performance management aspect of SLAs.

Y.1731 Scalability of

The following sections show the scaling numbers supported for :

Frame Delay and Frame-Delay Variation

The Frame Delay parameter can be used for on-demand OAM measurements of frame delay and frame-delay variation. When a maintenance end point (MEP) is enabled to generate frames with frame-delay measurement (ETH-DM) information, it periodically sends frames with ETH-DM information to its peer MEP in the same maintenance entity. Peer MEPs perform frame-delay and frame-delay variation measurements through this periodic exchange during the diagnostic interval.

An MEP requires the following specific configuration information to support ETH-DM:

- MEG level—MEG level at which the MEP exists
- Priority
- Transmission rate
- Total interval of ETH-DM

A MEP transmits frames with ETH-DM information using the TxTimeStampf information element. TxTimeStampf is the time stamp for when the ETH-DM frame was sent. A receiving MEP can compare the TxTimeStampf value with the RxTimef value, which is the time the ETH-DM frame was received, and calculate one-way delay using the formula *frame delay = RxTimef – TxTimeStampf*.

One-way frame-delay measurement (1DM) requires that clocks at both the transmitting MEP and the receiving MEPs are synchronized. Measuring frame-delay variation does not require clock synchronization and the variation can be measured using 1DM or a frame-delay measurement message (DMM) and a frame-delay measurement reply (DMR) frame combination.

If it is not practical to have clocks synchronized, only two-way frame-delay measurements can be made. In this case, the MEP transmits a frame containing ETH-DM request information and the TxTimeStampf element, and the receiving MEP responds with a frame containing ETH-DM reply information and the TxTimeStampf value copied from the ETH-DM request information.

Two-way frame delay is calculated as *(RxTimeb–TxTimeStampf)–(TxTimeStampb–RxTimeStampf)*, where RxTimeb is the time that the frame with ETH-DM reply information was received. Two-way frame delay and variation can be measured using only DMM and DMR frames.

To allow more precise two-way frame-delay measurement, the MEP replying to a frame with ETH-DM request information can also include two additional time stamps in the ETH-DM reply information:

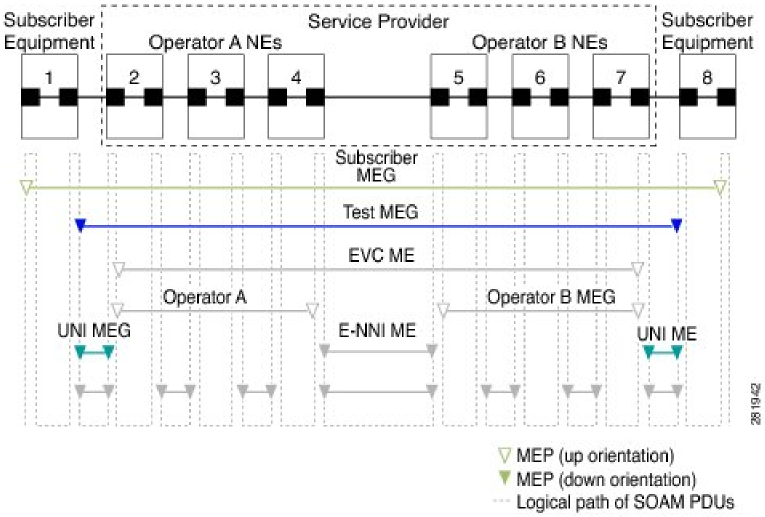
- RxTimeStampf—Time stamp of the time at which the frame with ETH-DM request information was received.
- TxTimeStampb—Time stamp of the time at which the transmitting frame with ETH-DM reply information was sent.
- The timestamping happens at the hardware level for DMM operations.

Note The frame-loss, frame-delay, and frame-delay variation measurement processes are terminated when faults related to continuity and availability occur or when known network topology changes occur.

An MIP is transparent to the frames with ETH-DM information; therefore, an MIP does not require information to support the ETH-DM function.

The figure below shows a functional overview of a typical network in which Y.1731 performance monitoring is used.

Figure 7: Y.1731 Performance Monitoring


Subscriber Equipment
Service Provider
Operator A NEs
Operator B NEs
Subscriber Equipment
1
2
3
4
5
6
7
8
Subscriber MEG
Test MEG
EVC ME
Operator A
Operator B MEG
UNI MEG
E-NNI ME
UNI ME
281942
MEP (up orientation)
MEP (down orientation)
Logical path of SOAM PDUs

Overview of Smart SFP

The smart SFP is a optical transceiver module that provides solutions for monitoring and troubleshooting Ethernet services using standardized protocols. It supports CFM and Y.1731 protocols as standalone device.

The Smart SFP maintains per vlan per cos statistics for all MEP configured on the router. When the Smart SFP receives a loss measurement (LM) frame matching a particular MEP, the statistics associated with particular MEP are inserted on the LM frame. To support performance management (PM), the router uses the Smart SFP to maintain per vlan per cos frame statistics and to add statistics and timestamps for PM frames when the local router is used as the source or the destination.

OAM functions described in ITU-T Y.1731 allow measurement of following performance parameters:

- Frame Delay and Frame Delay variation
- Frame Loss Ratio and Availability

Ethernet frame delay and frame delay variation are measured by sending periodic frames with ETH-DM (Timestamps) information to the peer MEP and receiving frames with ETH-DM reply information from the peer MEP. During the interval, the local MEP measures the frame delay and frame delay variation.

ETH-LM transmits frames with ETH-LM (frame counts) information to a peer MEP and similarly receives frames with ETH-LM reply information from the peer MEP. The local MEP performs frame loss measurements which contribute to unavailable time. A near-end frame loss refers to frame loss associated with ingress data frames. Far-end frame loss refers to frame loss associated with egress data frames.

To embed ETH-LM information on a LM frame, the platform should be capable of maintaining per vlan per cos statistics and insert this statistics into LM frames based on the vlan and cos present on the LM frame. This is performed by the Smart SFP on the router.

Connectivity

The first step to performance monitoring is verifying the connectivity. Continuity Check Messages (CCM) are best suited for connectivity verification, but is optimized for fault recovery operation. It is usually not accepted as a component of an SLA due to the timescale difference between SLA and Fault recovery. Hence, Connectivity Fault Management (CFM) and Continuity Check Database (CCDB) are used to verify connectivity. For more information on CFM, see Configuring Ethernet Connectivity Fault Management in a Service Provider Network.

IP SLA

IP Service Level Agreements (SLAs) for Metro-Ethernet gather network performance metrics in service-provider Ethernet networks. For more information on SLM or DM see *Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations*.

Configuring Loss Measurement Management

Loss Measurement Management (LMM) is a loss monitoring feature implemented using the Smart SFP. The LMM functionality is developed to monitor the loss and delay traffic measurement data on the router.

Configuring LMM

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet** *name*
5. **encapsulation** {**default** | **dot1q** | **priority-tagged** | **untagged**}
6. **bridge-domain** *bridge-id* [**split-horizon group** *group-id*]
7. **rewrite ingress tag pop** {**1** | **2**} **symmetric**
8. **xconnect** *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name*} **[sequencing** {**transmit** | **receive** | **both**}
9. **cfm mep domain** *domain-name* **mpid** *id*

10. **monitor loss counter priority** *value*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies the Gigabit Ethernet interface for configuration and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** *name* **Example:** `Device(config-if)# service instance 333 ethernet`	Configure an EFP (service instance) and enter service instance configuration) mode. • *id*—Specifies the number is the EFP identifier, an integer from 1 to 4000 • **ethernet** *name*—Specifies the name of a previously configured EVC. **Note** You do not need to use an EVC name in a service instance. **Note** The name should be the same as the evc name configured under the CFM domain **Note** Use service instance settings such as encapsulation, dot1q, and rewrite to configure tagging properties for a specific traffic flow within a given pseudowire session.
Step 5	**encapsulation** {**default** | **dot1q** | **priority-tagged** | **untagged**} **Example:** `Router (config-if-srv)# encapsulation dot1q 10`	Configure encapsulation type for the service instance. • **default**—Configure to match all unmatched packets. • **dot1q**—Configure 802.1Q encapsulation. See Encapsulation for details about options for this keyword. • **priority-tagged**—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7. • **untagged**—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.

	Command or Action	Purpose
Step 6	**bridge-domain** *bridge-id* [**split-horizon group** *group-id*] **Example:** `Router (config-if-srv)# bridge-domain 10`	Configure the bridge domain ID. The range is from 1 to 4000. You can use the **split-horizon** keyword to configure the port as a member of a split horizon group. The *group-id* range is from 0 to 2.
Step 7	**rewrite ingress tag pop** {**1** | **2**} **symmetric** **Example:** `Router (config-if-srv)# rewrite ingress tag pop 1 symmetric`	(Optional) Specify that encapsulation modification to occur on packets at ingress. • **pop 1**—Pop (remove) the outermost tag. • **pop 2**—Pop (remove) the two outermost tags. • **symmetric—**Configure the packet to undergo the reverse of the ingress action at egress. If a tag is popped at ingress, it is pushed (added) at egress. This keyword is required for **rewrite** to function properly.
Step 8	**xconnect** *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name*} **[sequencing** {**transmit** | **receive** | **both**} **Example:** `Router (config-if-srv)# xconnect 10.1.1.2 101 encapsulation mpls`	Binds the Ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC. **Note** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as ip route 10.30.30.2 255.255.255.255 10.2.3.4.
Step 9	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Router (config-if-srv)# cfm mep domain SSFP-2 mpid 2`	Configures the MEP domain and the ID.
Step 10	**monitor loss counter priority** *value* **Example:** `Router (config-if-srv)# monitor loss counter priority 0-7`	Configures monitor loss on the router. • **priority** *value*—Specifies the Cos value. the valid values are 0 to 7.
Step 11	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

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

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

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

Before you begin

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	- Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Device(config-term)# ip sla 11`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 loss** {**LMM** | **SLM**} [**burst**] **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **CoS** *CoS* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} **Example:** `Device(config-ip-sla)# ethernet y1731 loss LMM domain xxx vlan 12 mpid 34 CoS 4 source mpid 23`	Begins configuring a single-ended Ethernet frame loss ratio operation and enters IP SLA Y.1731 loss configuration mode. - 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. **Note** The session with mac-address will not be inactivated when there is CFM error.
Step 5	**aggregate interval** *seconds* **Example:** `Device(config-sla-y1731-loss)# aggregate interval 900`	(Optional) Configures the length of time during which performance measurements are conducted and the results stored.
Step 6	**availability algorithm** {**sliding-window** | **static-window**} **Example:** `Device(config-sla-y1731-loss)# availability algorithm static-window`	(Optional) Specifies availability algorithm used.
Step 7	**frame consecutive** *value* **Example:** `Device(config-sla-y1731-loss)# frame consecutive 10`	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status.

	Command or Action	Purpose
Step 8	**frame interval** *milliseconds* **Example:** `Device(config-sla-y1731-loss)# frame interval 100`	(Optional) Sets the gap between successive frames.
Step 9	**history interval** *intervals-stored* **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** *owner-id* **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	**exit** **Example:** `Device(config)# exit`	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.

Configuration Examples for LMM

- The following example shows a sample output of LMM:

Verifying LMM

- Use the **show ethernet cfm ma** {**local** | **remote**} command to display the loss on the MEP domain

```
Router# show ethernet cfm ma local

Local MEPs:
--------------------------------------------------------------------------------
MPID Domain Name                                 Lvl   MacAddress     Type  CC
Ofld Domain Id                                   Dir   Port           Id
     MA Name                                           SrvcInst       Source
     EVC name
--------------------------------------------------------------------------------
3    SSFP-3                                      3     0000.5c50.36bf XCON  Y
No   SSFP-3                                      Up    Gi0/1/4        N/A
     s3                                                3              Static
     e3
2    SSFP-2                                      2     0000.5c50.36bf XCON  Y
No   SSFP-2                                      Up    Gi0/1/4        N/A
     s2                                                2              Static
     e2
Total Local MEPs: 2
```

```
Router# show ethernet cfm ma remote

--------------------------------------------------------------------------------
MPID  Domain Name                                 MacAddress          IfSt  PtSt
 Lvl  Domain ID                                   Ingress
 RDI  MA Name                                     Type Id             SrvcInst
      EVC Name                                                        Age
      Local MEP Info
--------------------------------------------------------------------------------
20    SSFP-2                                      c471.fe02.9970      Up    Up
 2    SSFP-2                                      Gi0/1/4:(20.20.20.20, 2)
 -    s2                                          XCON N/A            2
      e2                                                              0s
      MPID: 2 Domain: SSFP-2 MA: s2
30    SSFP-3                                      c471.fe02.9970      Up    Up
 3    SSFP-3                                      Gi0/1/4:(20.20.20.20, 3)
 -    s3                                          XCON N/A            3
      e3                                                              0s
      MPID: 3 Domain: SSFP-3 MA: s3

Total Remote MEPs: 2
```

- Use the **show ip sla interval-stastistics** command to view the statistics.

```
Router# show ip sla history 3 interval-statistics

Loss Statistics for Y1731 Operation 3
Type of operation: Y1731 Loss Measurement
Latest operation start time: 09:19:21.974 UTC Mon Jan 20 2014
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  09:19:21.974 UTC Mon Jan 20 2014
 End time:  09:21:21.976 UTC Mon Jan 20 2014
 Number of measurements initiated: 120
 Number of measurements completed: 120
 Flag: OK
```

```
Forward
  Number of Observations 101
  Available indicators: 101
  Unavailable indicators: 0
  Tx frame count: 1000000
  Rx frame count: 1000000
    Min/Avg/Max - (FLR % ): 0:7225/000.00%/0:7225
  Cumulative - (FLR % ): 000.0000%
  Timestamps forward:
    Min - 09:21:08.703 UTC Mon Jan 20 2014
    Max - 09:21:08.703 UTC Mon Jan 20 2014
Backward
  Number of Observations 99
  Available indicators: 99
  Unavailable indicators: 0
  Tx frame count: 1000000
  Rx frame count: 1000000
    Min/Avg/Max - (FLR % ): 0:1435/000.00%/0:1435
  Cumulative - (FLR % ): 000.0000%
  Timestamps backward:
    Min - 09:21:08.703 UTC Mon Jan 20 2014
    Max - 09:21:08.703 UTC Mon Jan 20 2014
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

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

Feature Information for Loss Measurement Management (LMM) with Smart SFP

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

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

Table 4: Feature Information for Loss Measurement Management (LMM) with Smart SFP

Feature Name	Releases	Feature Information
Loss Measurement Management (LMM) with Smart SFP	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).

CHAPTER 9

IP SLA—Service Performance Testing

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

- Finding Feature Information, on page 75
- **Information About Service Performance Operations** , on page 75
- Information About Configuring Y.1564 to Generate and Measure Ethernet Traffic, on page 77
- Prerequisites for IP SLA - Service Performance Testing, on page 78
- Scale and Limitations for Configuring IP SLA - Service Performance Operation, on page 78
- Restrictions for IP SLA - Service Performance Operation, on page 79
- Generating Traffic Using Y.1564, on page 81
- How to Configure IP SLA - Service Performance Testing, on page 83
- Configuration Examples for Configuring Y.1564 to Generate and Measure Ethernet Traffic , on page 86
- Additional References for IP SLA - Service Performance Testing, on page 89

Finding Feature Information

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

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

Information About Service Performance Operations

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

Service performance testing is designed to measure the ability of a Device Under Test (DUT) or a network under test to forward traffic in different states.

Effective with Cisco IOS XE Everest Release 16.12.1, 10 Gigabit (10G) SAT Internal session is supported. Any SAT session with a rate-step greater than or equal to 1 Gbps is considered as 10G SAT session.

Cisco implementation of ITU-T Y.1564 has three key objectives:

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

The following Key Performance Indicators (KPI) metrics indicate the configured SLAs for the service or stream. These following service acceptance criteria metrics are:

- Information Rate (IR) or throughput—Measures the maximum rate at which none of the offered frames are dropped by the device under test (DUT). This measurement translates into the available bandwidth of the Ethernet virtual connection (EVC).
- Frame Loss Ratio (FLR)—Measures the number of packets lost from the total number of packets sent. Frame loss can be due to a number of issues such as network congestion or errors during transmissions.

Table 5: Supported Key Performance Indicators Matrix

KPI	**FPGA- Based SADT**	
Internal Direction	**External Direction**	
Delay	Y	Y
Jitter	Y	Y
Loss	Y	Y
Throughput	Y	Y

Note SADT Internal sessions do not support ASIC-based SAT.

Because they interconnect segments, forwarding devices (switches and routers) and network interface units are the basis of any network. Incorrect configuration of a service on any of these devices within the end-to-end path, can affect the network performance. This could also lead to potential service outages and network-wide issues such as congestion and link failures. Service performance testing is designed to measure the ability of DUT or network under test, to forward traffic in different states. The Cisco implementation of ITU-T Y.1564 includes the following service performance tests:

- Minimum data rate to CIR—Generates bandwidth from the minimum data rate to the committed information rate (CIR) for the test stream. Measures KPI for Y.1564 to meet configured service acceptance criteria (SAC).
- CIR to EIR—Ramps up bandwidth from the CIR to the excess information rate (EIR) for the test stream. Measures the transfer rate to ensure that CIR meets the minimum bandwidth of the maximum EIR. Other KPI is not measured.

Note In SADT configuration, if the rate of EIR is greater than CIR + EIR, then above EIR is not measured. The stats for *Above EIR* remains 0 in following command: **show ip sla statistics**

Service performance supports four operational modes:

- Two-way statistics collection
- One-way statistics collection
- Passive measurement mode
- Traffic generator mode

Statistics are calculated, collected, and reported to the IP SLAs module. The statistics database stores historical statistics pertaining to the operations that are executed.

- One-way statistics collection—Both the passive measurement mode and the traffic generator mode are used along with each other. One device sends traffic as the generator and another device receives traffic in the passive mode and records the statistics. The passive mode is distinct from the two-way mode, where the remote device records the statistics instead of looping back the traffic. The sending device records only the transmit statistics.
- Two-way statistics collection—The sender collects all the measurements. The remote target must be in the loopback mode for the two-way statistics to work. Loopback mode enables the traffic from the sender to reach the target and sent back to the sender.
- Passive measurement mode—This mode is enabled by excluding a configured traffic profile. A passive measurement operation does not generate live traffic. The operation collects only statistics for the target configured for the operation.
- Traffic generator mode—This mode records statistics for the number of packets and bytes transmitted.

Information About Configuring Y.1564 to Generate and Measure Ethernet Traffic

Y.1564 is an ethernet service activation or performance test methodology for turning up, installing, and troubleshooting ethernet and IP based services. This test methodology allows for complete validation of ethernet service-level agreements (SLAs) in a single test. Using the traffic generator performance profile, you can create the traffic based on your requirements. Network performance indicators like throughput, loss, and availability are analyzed using layer 2 traffic with various bandwidth profiles. Availability is inversely proportional to frame loss ratio.

The figure below shows the Traffic Generator topology describing the traffic flow in the external and internal modes. The traffic is generated at the wire-side of Network-to-Network Interface (NNI) and is transmitted to the responder through the same interface for the external mode. The traffic is generated at the User-to-Network Interface (UNI) and transmitted to the responder through NNI respectively for the internal mode. The external mode is used to measure the throughput and loss at the NNI port whereas internal mode is used to measure the throughput and loss at the UNI port. During traffic generation, traffic at other ports is not affected by the generated traffic and can continue to switch network traffic.

Effective from the Cisco IOS XE 16.12.x release, 10G SAT External is supported on the Cisco Router.

Prerequisites for IP SLA - Service Performance Testing

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

Scale and Limitations for Configuring IP SLA - Service Performance Operation

The following table lists the Y.1564 two-way throughput measurement.

Table 6: Y.1564 Throughput Measurement for Each Packet Size

Packet Size (Bytes)	Max Rate (kbps)
64	650000
128	820000
256	860000
512	860000
1024	880000
1280	900000
1518	970000
9216	980000

Note Higher order 1-GigabitEthernet ports and 10-GigabitEthernet port could have few packet loss in 9216 packet size. The above measurements are taken with external mode. Measured throughput value could be higher than configured rate upto 2%.

Traffic Generator

- Supports eight simultaneous transmit sessions on device with a maximum rate of 1 Gbps .
- Supports color-blind traffic generation.
- SAT traffic is always generated in a burst.

Default q-limit values are not adequate to handle the burst and thus leading to packet drops. You need to use the **platform qos-qlimit-disable** command to disable q-limit on the router and this would enable dynamic sharing of resources on all ports.

The **platform qos-qlimit-disable** command disables the QoS q-limit functionality and enables the functionality again once the **platform qos-qlimit-disable** command is removed.

Measurement

The default ether-type to configure SAT endpoint is 0x8904. The measurement can only match packets with ether-type of 0x8904.

NCS 520 traffic generation happens with ether-type of 0x8904 by default. The measurement works if the traffic generator is also NCS 520 or its two-way statistics. The measurement cannot be used if there are devices other than NCS 520 on the other side as the traffic generator. Ether-types IPv4 and IPv6 are user configurable option (ether-type) supported. With the configuration set, you can perform measurement of packets from other devices with ether-type as IPv4 or IPv6.

SAT on NCS520 is supported only for Ethernet mode.

Loopback

NCS 520 does not support ethernet loopback or latching loopback.

NCS 520 supports loopback on SAT, and IP SLA configuration itself is used.

Use the **loopback direction** for the session along with packet profile. Source MAC address and destination MAC address are not same for loopback session. If an IP SLA session is configured as loopback mode, then the session should not have measurement or traffic profile parameters, otherwise the configuration fails.

Loopback sessions does not support statistics.

Restrictions for IP SLA - Service Performance Operation

- Layer 3 fields such as IP, DSCP, and Layer 4 ports are not supported as packet parameter.
- Measurement is supported only for throughput and loss. Delay and jitter measurement are not supported.
- Service types are supported only for EFPs and not for bridge-domain and Layer 3 interfaces.
- Maximum number of sessions supported is 8 and these 8 sessions can run simultaneously.
- Color aware statistics is not supported.
- Port-channel testing is not supported.
- When a configuration performed on EFP or interface is shutdown, the packets do not egress out of any interface on the device, and after unshut, the traffic does not resume to egress direction. You need to restart the configuration manually.
- On test EFP or BD removal on the test interface, traffic does not egress out of any of the interfaces in the device, and traffic flow resumes only after reconfiguring. After which, the test is rescheduled.
- Each session should have an unique encapsulation, and if sessions have same encapsulations or match keys might impact the statistics.
- Packets that use SAT internal MAC (0xf244493930ec) as destination MAC addresss and internal VLAN (0xdd4) have problem with forwarding.

- Loopback or measurement with packet size of 1518 at ingress direction does not work. This is due to the extra headers being added at ingress direction. To overcome this, MTU size of the interface has to be increased.
- Span on the SAT configured interface is not supported.

  Rx statistics work only after 10 seconds and you need to use the **platform qos-qlimit-disable** command to disable the q-limit on the router before starting the SLA session.
- SLA measurement in 10-Gigabit Ethernet port is supported with maximum rate of 1-Gigabit Ethernet. Higher the order of 1-Gigabit Ethernet ports, 10-Gigabit Ethernet ports have few packets loss for higher packet size.
- Interface statistics and SLA statistics might not match in higher order ports.
- The following table shows the supported egress and ingress QOS on the sender side core interface for Ethernet and IP target SLA.

Table 7: IP SLA and Type of QOS supported

Type	Policy-map at interface (Ingress)	Policy-map at interface (Egress)	Policy-map at EFP (Ingress)	Policy-map at EFP (Egress)
Internal Mode 2-way measurement	Yes	Yes	Yes	Yes
Internal Receive Mode	No	Yes	No	Yes
Internal Loopback Target Interface	Yes	Yes	Yes	Yes
External Mode 2-way measurement	No	No	No	No
External Receive Mode	Yes	No	Yes	No
External Loopback Target Interface	Yes	No	Yes	No

Note Ingress classification does not work for match on VLAN for SADT traffic.

- The following table shows how Ethernet Target SLA with multicast or broadcast source MAC address is supported on different operational modes.

Table 8: Multicast or Broadcast MAC support criteria for SLA

Source or destination MAC address	Operational mode	Support for Ethernet Target SLA
Multicast or broadcast source MAC address	Traffic generator mode	Not supported
	Passive measurement mode	
	Two-way statistics collection mode	
Multicast or broadcast destination MAC address	Traffic generator mode	SLA generates the traffic
	Passive measurement mode	SLA receives the traffic
	Two-way statistics collection mode	Not supported

Generating Traffic Using Y.1564

Follow these steps to generate traffic using Y.1564:

SUMMARY STEPS

1. Configure Ethernet Virtual Circuits (EVC).
2. Configure Traffic Generator on the transmitter.
3. Configure loopback on SAT IP SLA configuration itself at the remote end.
4. Configure loopback on SAT IP SLA configuration itself, if remote end is NCS 520 or use ether-type as IPv4 or IPv6, if remote node is other than NCS520.
5. Start the IP SLA session:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure Ethernet Virtual Circuits (EVC).	EVC is configured on the interface path such that the layer 2 path between the transmitter and the receiver is complete. For more information, see the "Configuring Ethernet Virtual Connections (EVCs)" section in the *Carrier Ethernet Configuration Guide, Cisco IOS XE Release* .
Step 2	Configure Traffic Generator on the transmitter. **Example:** The following is a sample configuration of the traffic generator.	

```
Direction - External
ip sla 200
service-performance type ethernet dest-mac-addr
```

	Command or Action	Purpose

```
0000.0300.0301 interface GigabitEthernet 0/0/1
service instance 300
frequency iteration 1 delay 1
duration time 50
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
packet-size 256
profile traffic direction external
rate-step kbps 50000
Direction - Internal
ip sla 200
service-performance type ethernet dest-mac-addr
0000.0300.0301 interface GigabitEthernet 0/0/1
service instance 300
frequency iteration 1 delay 1
duration time 50
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
packet-size 256
profile traffic direction internal
rate-step kbps 50000
```

Step 3

Configure loopback on SAT IP SLA configuration itself at the remote end.

Example:

```
ip sla 1
 service-performance type ethernet dest-mac-addr
0001.0001.0001 interface GigabitEthernet0/0/3
service instance 2
  loopback direction external
  profile packet
   inner-vlan 20
   outer-vlan 10
   src-mac-addr 0002.0002.0002
  duration time 5000
```

Step 4

Configure loopback on SAT IP SLA configuration itself, if remote end is NCS 520 or use ether-type as IPv4 or IPv6, if remote node is other than NCS520.

Step 5

Start the IP SLA session:

Example:

```
Router(config)# ip sla schedule [sla_id] start-time
 [hh:mm | hh:mm:ss | now | pending | random]
```

How to Configure IP SLA - Service Performance Testing

Y.1564 support on dot1ad Encapsulation

Table 9: Feature History

Feature Name	Release Information	Feature Description
Y.1564 support on dot1ad	Cisco IOS XE Cupertino 17.8.1	This feature enables Y.1564 Ethernet service activation test methodology support on interfaces that are configured with 802.1ad encapsulation. It allows you to perform medium-term and long-term service testing, confirming that the interfaces that are configured with 802.1ad can properly carry all services while under stress during a soaking period. The following commands are introduced: - **inner-eth-type** - **outer-eth-type**

Configuring Ethernet Target Two-Way Color Blind Session

Perform the following steps to configure ethernet target color blind traffic generation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *sla_id*
4. **service-performance type ethernet dest-mac-addr** *dest-mac* **service instance**
5. **aggregation** | **default** | **description** | **duration** | **exit** | **frequency** | **no** | **profile**
6. **measurement-type direction** {**internal** | **external**}
7. **default** | **exit** | **no** | **throughput** | **receive**
8. **exit**
9. **profile packet**
10. **default** | **exit** | **inner-cos** | **inner-vlan** | **no** | **outer-cos** | **outer-vlan** | **packet-size** | **src-mac-addr** | **outer-eth-type** | **inner-eth-type**
11. **exit**
12. **profile traffic direction**{**external** | **internal**}
13. **default** or **exit** or **no** or **rate step kbps** | **pps**

14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *sla_id* **Example:** `Device(config)# ip sla 100`	Specifies the SLA ID to start the IP SLA session.

Step 4	**service-performance type ethernet dest-mac-addr** *dest-mac* **service instance**
	Example:
	`Device(config-ip-sla))#service-performance type`
	`ethernet dest-mac-addr 0001.0001.0001 interface`
	`gigabitEthernet0/10 service instance 10`
		Specifies the service performance type as Ethernet and the destination MAC address in H.H.H format.
		Specifies the target for the SLA session. The options is service instance.

Step 5	**aggregation** | **default** | **description** | **duration** | **exit** | **frequency** | **no** | **profile**
	Example:
	`Device(config-ip-sla-service-performance)#`
	`duration time 60`
		Specifies the type of service performance. The options are:
		• **aggregation** - Represents the statistics aggregation.
		• **default** - Sets a command to its defaults.
		• **description** - Describes the operation.
		• **duration** - Sets the service performance duration configuration.
		• **frequency** - Represents the scheduled frequency. The options available are iteration and time. The range in seconds is from 20 to 65535.
		• **profile** - Specifies the service performance profile. If you use the packet or traffic options, go to Step 9 or Step 12, respectively.

Step 6	**measurement-type direction** {**internal** | **external**}
	Example:
	`Device(config-ip-sla-service-performance)#`
	`measurement-type direction`
		Specifies the statistics to measure traffic. The options available are external or internal; the default option is internal.
		Only external measurement-type direction is supported for 10G.

Step 7	**default** | **exit** | **no** | **throughput** | **receive** **Example:**	Specifies the measurement type based on the service performance is calculated. The options are:

	Command or Action	Purpose
	`Device(config-ip-sla-service-performance-measurement)# throughput`	- **default** - Sets a command to its defaults. - **throughput** - Specifies the measurement such as average rate of successful frame delivery. - **receive** - Specifies the passive measurement mode.
Step 8	**exit**	Exits the measurement mode.
Step 9	**profile packet** **Example:** `Device(config-ip-sla-service-performance)#profile packet`	Specifies the packet profile. A packet profile defines the packets to be generated.
Step 10	**default** | **exit** | **inner-cos** | **inner-vlan** | **no** | **outer-cos** | **outer-vlan** | **packet-size** | **src-mac-addr** | **outer-eth-type** | **inner-eth-type** **Example:** `Device(config-ip-sla-service-performance-packet)#src-mac-addr 4055.3989.7b56`	Specifies the packet type. The options are: - **default** - Sets a command to its defaults. - **inner-cos** - Specifies the class of service (CoS) value for the inner VLAN tag of the interface from which the message will be sent. - **inner-vlan** - Specifies the VLAN ID for the inner vlan tag of the interface from which the message will be sent. - **outer-cos** - Specifies the CoS value that will be populated in the outer VLAN tag of the packet. - **outer-vlan** - Specifies the VLAN ID that will be populated in the outer VLAN tag of the packet. - **packet-size** - Specifies the packet size; the default size is 64 bytes. The supported packet sizes are 64 bytes,128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, 1518 bytes, and 9216 bytes. - **src-mac-addr** - Specifies the source MAC address in H.H.H format. - **outer-eth-type** - Specifies the encapsulation type for the outer VLAN tag of the packet as dot1ad or dot1q. - **inner-eth-type** - Specifies the encapsulation type for the inner VLAN tag of the interface from which the message is sent as dot1ad or dot1q. **Note** Ensure that the value of the configured packet profile matches the target configuration of the session. **Note** If you do not specify the encapsulation type in the packet profile, `dot1q` is used by default.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)# exit`	Exits the packet mode.
Step 12	**profile traffic direction**{**external** | **internal**} **Example:** `Device(config-ip-sla-service-performance)#profile traffic direction external`	Specifies the direction of the profile traffic. The options are external and internal. **Note** This command is required to configure the **rate step kbps** command.
Step 13	**default** or **exit** or **no** or **rate step kbps | pps** **Example:** `Device(config-ip-sla-service-performance-traffic)#rate-step kbps 1000`	Specifies the traffic type. The options are: • **default** - Sets a command to its defaults. • **rate step kbps** - Specifies the transmission rate in kbps. The rate-step range is from 1-10000000 (1 Kbps to 10 Gbps). • **rate step pps** - Specifies the transmission rate in pps. The rate-step range is from 1-1000000 (1 to 1000000 pps). **Note** The command **rate-step kbps | pps number** is mandatory for traffic generation.
Step 14	**exit**	Exits the traffic mode.

Configuration Examples for Configuring Y.1564 to Generate and Measure Ethernet Traffic

This section shows sample configurations for traffic generation.

Example: Traffic Generation

This section shows sample configuration for traffic generation – target service instance.

```
Direction - External
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0300.0301 interface GigabitEthernet
0/0/1 service instance 300
frequency iteration 1 delay 1
duration time 50
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
packet-size 256
```

```
profile traffic direction external
rate-step kbps 50000
Direction - Internal
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0300.0301 interface GigabitEthernet
0/0/1 service instance 300
frequency iteration 1 delay 1
duration time 50
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
packet-size 256
profile traffic direction internal
rate-step kbps 50000
```

Example: Two-Way Session

The following is a sample configuration for a two-way measurement session.

Two-way measurement mode: Direction - Internal

```
ip sla 12345
service-performance type ethernet dest-mac-addr 00ab.cdef.1234 interface
TenGigabitEthernet0/0/4 service instance 1000
measurement-type direction internal
receive
throughput
profile packet
outer-cos 2
outer-vlan 999
packet-size 1518
src-mac-addr 0012.3456.789a
profile traffic direction internal
rate-step kbps 10000 15000
duration time 100
```

Two-way measurement mode: Direction - External

```
ip sla 12345
service-performance type ethernet dest-mac-addr 00ab.cdef.1234 interface
TenGigabitEthernet0/0/4 service instance 1000
measurement-type direction external
receive
throughput
profile packet
outer-cos 2
outer-vlan 999
packet-size 1518
src-mac-addr 0012.3456.789a
profile traffic direction external
rate-step kbps 10000 15000
```

Example: Passive Measurement Mode

The following is a sample configuration for passive measurement session.

Direction - External

```
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0300.0301 interface GigabitEthernet
0/0/11 service instance 300
measurement-type direction external
receive
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
packet-size 256
```

Direction - Internal

```
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0300.0301 interface GigabitEthernet
0/0/11 service instance 300
measurement-type direction internal
receive
profile packet
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
packet-size 256
```

Example: Two-Way Measurement Mode

The following is a sample loopback configuration for a two-way measurement mode.

Direction - External:

```
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0300.0301 interface GigabitEthernet
0/0/11 service instance 300
measurement-type direction external
receive
profile packet
inner-cos 5
outer-cos 5
inner-vlan 101
outer-vlan 101
```

Direction - Internal:

```
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0300.0301 interface GigabitEthernet
0/0/11 service instance 300
measurement-type direction internal
receive
profile packet
profile packet
inner-cos 5
outer-cos 5
```

```
inner-vlan 101
outer-vlan 101
```

Additional References for IP SLA - Service Performance Testing

Related Documents

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

Standards and RFCs

Standard/RFC	Title
ITU-T Y.1564	*Ethernet service activation test methodology*

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