IP SLAs Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)

First Published: 2019-11-14

Last Modified: 2023-03-31

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

CONTENTS

CHAPTER 1 **Feature History** 1

CHAPTER 2 **IP SLAs Overview** 3

- Information About IP SLAs 3
  - IP SLAs Technology Overview 3
  - Service Level Agreements 4
  - Benefits of IP SLAs 5
  - Restriction for IP SLAs 6
  - Network Performance Measurement Using IP SLAs 6
  - IP SLAs Responder and IP SLAs Control Protocol 7
  - Response Time Computation for IP SLAs 8
  - IP SLAs Operation Scheduling 8
  - IP SLAs Operation Threshold Monitoring 9
  - History Statistics 9
- Additional References 10

CHAPTER 3 **Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations** 11

- Prerequisites for ITU-T Y.1731 Operations 11
- Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) 11
- How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 12
  - Configuring a Dual-Ended Ethernet Delay or Delay Variation Operation 12
    - Configuring a Receiver MEP on the Destination Device 12
    - Configuring the Sender MEP on the Source Router 14
  - Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation 16
  - Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation 19
  - Scheduling IP SLAs Operations 21

Enabling NTP Time of Day Synchronization 23
Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 24
Example: Dual-Ended Ethernet Delay Operation 24
Example: Frame Delay and Frame Delay Variation Measurement Configuration 25
Example: Sender MEP for a Single-Ended Ethernet Delay Operation 26
Example: Sender MEP for a Single-Ended Ethernet Frame Loss Operation 26
Example: Verifying NTP Time Of Day Synchronization 27
Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 27
Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations 29

CHAPTER 4 **IPSLA Y1731 On-Demand and Concurrent Operations** 31
Prerequisites for ITU-T Y.1731 Operations 31
Restrictions for IP SLAs Y.1731 On-Demand Operations 31
Information About IP SLAs Y.1731 On-Demand and Concurrent Operations 32
IPSLA Y1731 SLM Feature Enhancements 32
How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations 33
Configuring a Direct On-Demand Operation on a Sender MEP 33
Configuring a Referenced On-Demand Operation on a Sender MEP 34
Configuring an IP SLAs Y.1731 Concurrent Operation on a Sender MEP 34
Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations 34
Example: On-Demand Operation in Direct Mode 34
Example: On-Demand Operation in Referenced Mode 36
Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations 37
Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations 38

CHAPTER 5 **IP SLAs TWAMP Responder** 41
NTP and PTP time stamping for TWAMP test packet 41
Prerequisites for IP SLAs TWAMP Responder 42
Restrictions for IP SLAs TWAMP Responder 42
IP SLAs TWAMP Architecture 42
Two-Way Active Measurement Protocol (TWAMP) 42
IP SLAs TWAMP Responder 43
Two-Way Active Measurement Protocol 44
Configure an IP SLAs TWAMP Responder 45

Configuring the TWAMP Server 46
Configuring the Session Reflector 47
Configuration Examples for IP SLAs TWAMP Responder 48
Configuration Example for IP SLAs TWAMP Responder 48
IP SLAs TWAMP Light 49
Restrictions for IP SLAs TWAMP Light 50
Configuring TWAMP Light 50
Verifying TWAMP Light 51
Additional References 51
Feature Information for IP SLAs TWAMP Responder 52

CHAPTER 6 **ITU-T Y.1731 Performance Monitoring in a Service Provider Network** 53
Prerequisites for ITU-T Y.1731 Performance Monitoring in a Service Provider Network 53
Restrictions for ITU-T Y.1731 Performance Monitoring in a Service Provider Network 54
Information About ITU-T Y.1731 Performance Monitoring in a Service Provider Network 54
Frame Delay and Frame-Delay Variation 54
Benefits of ITU-T Y.1731 Performance Monitoring 56
How to Configure ITU-T Y.1731 Performance Monitoring in a Service Provider Network 56
Configuring Performance Monitoring Parameters 56
Configuration Examples for Configuring ITU-T Y.1731 Performance Monitoring Functions 57
Example: Configuring Performance Monitoring 57
Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network 57

CHAPTER 7 **Configuring an SLM** 59
Configuring SLM over VPLS 59
Restrictions for SLM support over VPLS 60
Configuring an SLM 60
Scheduling an IP SLA Operation 64
Configuration Example for SLM over VPLS 65

CHAPTER 8 **Configuring DMM over VPLS** 67
Restrictions for DMM support over VPLS 67
Configuring DMM over VPLS 67
Configuration Example for DMM over VPLS 68

Configuration Verification Example for DMM over VPLS 69

CHAPTER 9 **Configuring Loss Measurement Management** 71
Prerequisites for LMM 71
Restrictions for Smart SFP 71
Information About Loss Measurement Management (LMM) 72
Y.1731 Performance Monitoring (PM) 72
ITU-T Y.1731 Performance Monitoring in a Service Provider Network 73
Y.1731 Scalability of ASR 920 73
Frame Delay and Frame-Delay Variation 73
Overview of Smart SFP 75
Connectivity 75
IP SLA 76
Configuring Loss Measurement Management 76
Configuring LMM 76
Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation 78
Configuration Examples for LMM 81
Verifying LMM 81
Additional References 83
Feature Information for Loss Measurement Management (LMM) with Smart SFP 83

CHAPTER 10 **IP SLA—Service Performance Testing** 85
Information About Service Performance Operations 85
Prerequisites for IP SLA - Service Performance Testing 87
Restrictions for IP SLA - Service Performance Operation 87
Restrictions on the Cisco ASR 920 Routers 89
Restrictions for FPGA Based SAT 92
Information About Configuring Y.1564 to Generate and Measure Ethernet Traffic 93
Scale and Limitations for Configuring IP SLA - Service Performance Operation 94
Generating Traffic Using Y.1564 96
How to Configure IP SLA - Service Performance Testing 98
Configuring Ethernet Target Two-Way Color Blind Session 98
Configuring Ethernet Target Color-Aware Traffic Generation 102
Configuring Ethernet Target Two-Way Color-Aware Session 105

Configuring Ethernet Target Passive Color-Aware Measurement 109

Configuring Ethernet Target for Color-Aware Traffic Generation with IMIX 112

Configuring Y.1564 Traffic payload pattern 115

Configuration Examples for Configuring Y.1564 to Generate and Measure Ethernet Traffic 116

Example: Traffic Generation — Target Service Instance 116

Example: Traffic Generation — Target Bridge Domain 116

Example: Two-Way Session—Target Service Instance 116

Example: Two-Way Session — Target Bridge Domain 117

Example: Passive Measurement Mode — Target Service Instance 117

Example: Passive Measurement Mode — Target Bridge Domain 118

Example: Traffic Generation Mode — Color Aware 118

Example: Traffic Generation Mode with IMIX — Color Aware 118

Example: Two-way Color-Aware Measurement Session 118

Example: Passive Color-Aware Measurement Session 119

Example: Two-Way Session 119

Example: 10G Ethernet Two-Way Color Blind Session 119

How to Configure Y.1564 to Generate and Measure IP Traffic 120

Configuring IP Target Color-Aware Traffic Generation 121

Configuring IP Target Color Blind Traffic Generation 124

Configuring IP Target Color Blind Passive Measurement 126

Configuring IP Target Two-Way Color-Aware Session 128

Configuring IP Target Color-Aware IMIX Traffic Generation 132

Configuration Examples for Configuring Y.1564 t o Generate and Measure IP Traffic 135

Example: Passive Color-Aware Measurement Session 135

Example: Color-Aware IMIX — Traffic Generation 135

Example: Color-Aware — Traffic Generation 136

Example: Color Blind — Traffic Generation 136

Example: Color Blind — Passive Measurement 136

Example: Color-Aware — Two Way 137

Example: Color Blind — Two Way 137

Example: Configuring Y1564 Traffic Payload Pattern 137

How to Configure IP (Layer 3) Loopback on Responder 138

Enabling IP SLA Loopback on Responder 138

SADT Overhead Accounting 140

Restrictions 141
Configuring SADT Overhead Accounting 142
Verifying SADT Overhead Accounting Configuration 142
Configurable User-Defined and EMIX Packet Size 142
Configuration Example: Configurable User-Defined and EMIX Packet Size 144
Verification of User-Defined and EMIX Packet Size Configuration 145
SADT over VC When Access Interface is Down 146
Limitations for SADT Over VC Feature 146
Configuring SADT and Pseudowire Circuit 146
Verifying SADT and Pseudowire Circuit 147
Additional References for IP SLA - Service Performance Testing 148

CHAPTER 11 **IP SLA VCCV Operation** 151
Configuring and Scheduling an IP SLA VCCV Operation 151
Example for Configuring an IP SLA VCCV Operation 154

CHAPTER 1

Feature History

The following table lists the new and modified features supported in the IP SLAs Configuration Guide in Cisco IOS XE 17 releases.

Feature	Description
Cisco IOS XE Dublin 17.10.1	
SADT over VC when Access Interface is Down	You can perform Service Activation and Deactivation (SADT) over Virtual Circuit (VC) even when access interface is down.
Cisco IOS XE Bengaluru 17.5.1	
TWAMP Light	This feature enables you to configure a TWAMP Light session using the ip **`sla responder twamp-light test-session`** command on the Cisco RSP2 module.
Cisco IOS XE Bengaluru 17.4.1	
Configurable User-Defined and EMIX Packet Size	This feature allows you to configure user-defined and Enterprise traffic (EMIX) packet sizes. Use the following commands to configure user-defined and EMIX packet sizes: • **packet-size user-defined** *packet size* • **packet-size emix-sequence** *emix-sequence* [**u-value** *u-value value*]
EMIX Sequence Enhancement	This feature enables SAT based support for configurable EMIX traffic pattern in FPGA-based SAT.
SAT based support for configurable EMIX traffic pattern in FPGA	The support for EMIX packet size is enhanced. For EMIX traffic, packet sizes of 64, 128, 256, 512, 1024, 1280, 1518, Maximum Transmission Unit (MTU) and user-defined patterns are supported. These packet sizes are forwarded in ratio of 1:1:1:1:1.
Cisco IOS XE Amsterdam 17.3.1	
Configurable Y.1564 Service Activation Frame Sizes and EMIX Support	Starting with Cisco IOS XE Amsterdam 17.3.1 release, EMIX packet size is supported. For EMIX traffic, packet sizes of 64, 128, 256, 1024 and 1518 bytes are supported. These packet sizes are forwarded in ratio of 1:1:1:1:1.

CHAPTER 2

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 3
- Additional References, on page 10

Information About IP SLAs

IP SLAs Technology Overview

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

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

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

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

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

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

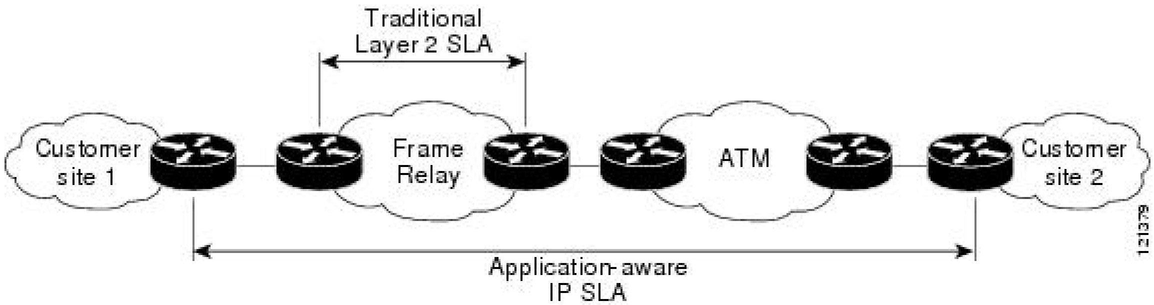
SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and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

Service Level Agreements

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

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

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



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

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

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

Benefits of IP SLAs

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

  - Provides proactive verification and connectivity testing of network resources (for example, indicates the network availability of a Network File System (NFS) server used to store business critical data from a remote site).

- Troubleshooting of network operation
  - Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.

- Voice over IP (VoIP) performance monitoring
- Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) performance monitoring and network verification

Restriction for IP SLAs

- With *SR_5_label_push* template, IP SLA DMM is not supported on RSP3 module.
- The maximum supported scale number of CFM and IP SLA over the port channel is only 300.
- IP SLAs configured with *start-time now* keyword need to be restarted after reload.
- IP SLA v1, v2, v3 do not support HMAC SHA 1, HMCA SHA 256, HMCA SHA 384, HMCA SHA 512 authentications on the routers.
- IP SLA statistics gets suppressed when you configure the rate step 1000000 kbps. The rate step value should not be equal or greater than 1G.

Note This is applicable to 1G SADT only; rate step equal to 1000000 kbps or greater is treated as 10G SADT.

- When EFP is configured with encapsulation by default, the packet is not encapsulated with the vlan header. As a result, the CoS value is zero and the IP SLA session is not completed.

Network Performance Measurement Using IP SLAs

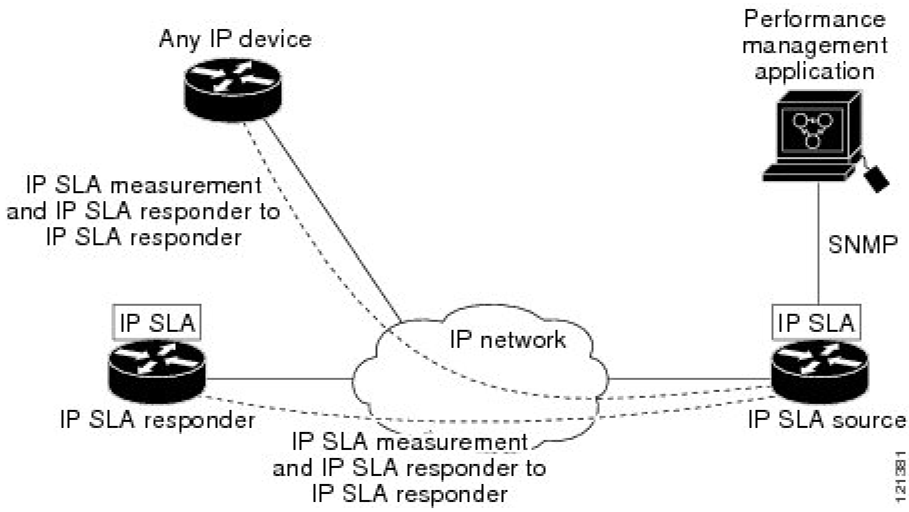
Using IP SLAs, a network engineer can monitor the performance between any area in the network: core, distribution, and edge. Monitoring can be done anytime, anywhere, without deploying a physical probe.

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

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

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

Figure 2: IP SLAs Operations



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

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

IP SLAs Responder and IP SLAs Control Protocol

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

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

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

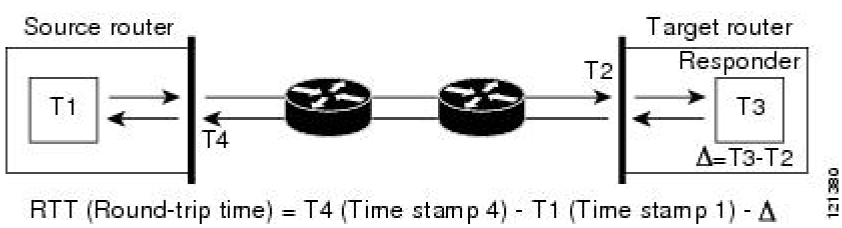
Response Time Computation for IP SLAs

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

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

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

Figure 3: IP SLAs Responder Time Stamping



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

IP SLAs Operation Scheduling

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

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

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

IP SLAs Operation Threshold Monitoring

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

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

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

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

History Statistics

IP SLAs maintains the following three types of history statistics:

- Aggregated statistics--By default, IP SLAs maintains two hours of aggregated statistics for each operation. Value from each operation cycle is aggregated with the previously available data within a given hour. The Enhanced History feature in IP SLAs allows for the aggregation interval to be shorter than an hour.
- Operation snapshot history--IP SLAs maintains a snapshot of data for each operation instance that matches a configurable filter, such as all, over threshold, or failures. The entire set of data is available and no aggregation takes place.
- Distribution statistics--IP SLAs maintains a frequency distribution over configurable intervals. Each time IP SLAs starts an operation, a new history bucket is created until the number of history buckets matches the specified size or the lifetime of the operation expires. By default, the history for an IP SLAs operation

is not collected. If history is collected, each bucket contains one or more history entries from the operation. History buckets do not wrap.

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

CHAPTER 3

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

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

- Ethernet Delay
- Ethernet Delay Variation
- Ethernet Frame Loss Ratio

- Prerequisites for ITU-T Y.1731 Operations, on page 11
- Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731), on page 11
- How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations, on page 12
- Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations, on page 24
- Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations , on page 27
- Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations, on page 29

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.

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config-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 5000,10000,15000,20000,-1`	(Optional) Specifies measurement type and configures bins for statistics distributions kept. Allowed number of bin upper boundaries : 9
Step 7	**frame offset** *offset-value* **Example:** `Router(config-sla-y1731-delay)# frame offset 1`	(Optional) Sets the value for calculating delay variation rates.

	Command or Action	Purpose
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.

Procedure

	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.
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.

	Command or Action	Purpose
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.

Procedure

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Device(config-term)# ip sla 10`	Begins 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. **Note** In the case of an interface or MEP flap, the Y.1731 session recovery takes the default aggregate interval value of 900 seconds. Decrease this value for a faster recovery of the session.

	Command or Action	Purpose
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. Allowed number of bin upper boundaries : 9
Step 8	**frame interval** *milliseconds* **Example:** `Device(config-sla-y1731-delay)# frame interval 100`	(Optional) Sets the gap between successive frames.
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.

	Command or Action	Purpose
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.

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Device(config-term)# ip sla 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 (,).

Procedure

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

Step 3	Enter one of the following commands:
	• **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
	• **ip sla group schedule** *group-operation-number operation-id-numbers* {**schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
	Example:
	`Device(config)# ip sla schedule 10 life forever start-time now`
	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`
		• Configures the scheduling parameters for an individual IP SLAs operation.
		• Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

Step 4	**end** **Example:**	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	
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.

Procedure

	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

Related Topic	Document Title
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 4

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 31
- Restrictions for IP SLAs Y.1731 On-Demand Operations, on page 31
- Information About IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 32
- How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 33
- Configuration Examples for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 34
- Additional References for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 37
- Feature Information for IP SLAs Y.1731 On-Demand and Concurrent Operations, on page 38

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.

Procedure

	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:** `Device# ip sla on-demand ethernet SLM domain xxx vlan 12 mpid 34 cos 4 source mpid 23 continuous aggregation 10 duration 60`	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.

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*.

Procedure

	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
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*

Related Topic	Document Title
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 5

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.

- NTP and PTP time stamping for TWAMP test packet, on page 41
- Prerequisites for IP SLAs TWAMP Responder, on page 42
- Restrictions for IP SLAs TWAMP Responder, on page 42
- IP SLAs TWAMP Architecture, on page 42
- Configure an IP SLAs TWAMP Responder, on page 45
- Configuration Examples for IP SLAs TWAMP Responder, on page 48
- IP SLAs TWAMP Light, on page 49
- Additional References, on page 51
- Feature Information for IP SLAs TWAMP Responder, on page 52

NTP and PTP time stamping for TWAMP test packet

- To enable NTP time stamping for TWAMP test packet, run the following commands:
  - If TWAMP sender has epoch 1900 clock reference, enable the **platform time-source ntp time-scale epoch-1900** command.
  - If TWAMP sender has epoch 1970 clock reference, enable the **platform time-source ntp time-scale epoch-1970** command.

Table 3: Feature History

Feature Name	Release Information	Description
PTP time stamping	Cisco IOS XE Cupertino 17.9.1	Starting with Cisco IOS XE 17.9.x, TWAMP with PTP time stamping is supported.

- To enable PTP time stamping for TWAMP test packet, run the following commands:
  - If you need time stamps with leap seconds granularity, enable the **platform twamp_ptp_utc_time_scale_epoch_1900** command.
  - If you need time stamps without leap seconds granularity, enable the **platform twamp_ptp_time_scale_epoch_1900** command.

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 routed interfaces and BDI interfaces.
- TWAMP client and session sender are not supported.
- Effective Cisco IOS XE Bengaluru 17.5.1 TWAMP Light mode is supported.

  TWAMP Light mode is not supported in releases pror to Cisco IOS XE Bengaluru 17.5.1 release.
- Custom DSCP values are not supported on TWAMP. The DSCP values used in the control phase are populated in the TWAMP test packets irrespective of whatever may be the DSCP value in the test packets incoming to the reflector.

IP SLAs TWAMP Architecture

Two-Way Active Measurement Protocol (TWAMP)

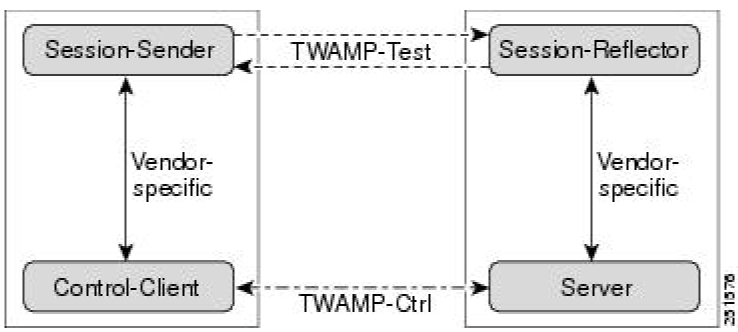
The IETF Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the TWAMP protocols. The TWAMP-Control protocol is used to set up performance measurement sessions. The TWAMP-Test protocol is used to send and receive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

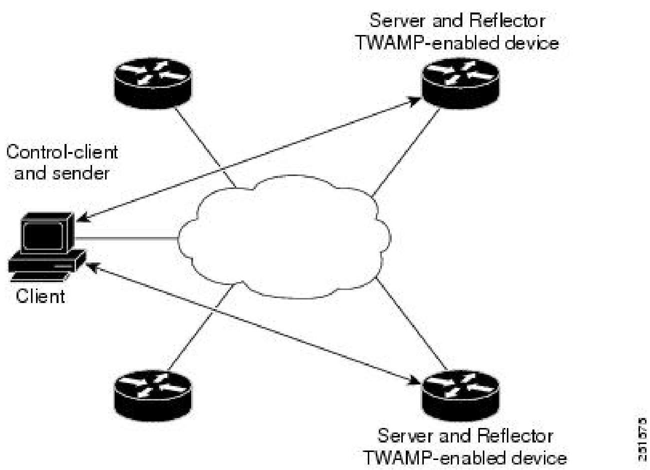


IP SLAs TWAMP Responder

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



Note ASR 920 supports only hardware time stamping.

Two-Way Active Measurement Protocol

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

- Advantages of TWAMP, on page 44
- The TWAMP entities, on page 44
- TWAMP Message Exchange Categories, on page 45

Advantages of TWAMP

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

The TWAMP entities

The TWAMP system consists of four logical entities:

- server -- manages one or more TWAMP sessions and also configures per-session ports in the end-points.
- session-reflector - reflects a measurement packet as soon as it receives a TWAMP test packet.
- control-client - initiates the start and stop of TWAMP test sessions.
- session-sender - instantiates the TWAMP test packets sent to the session reflector.

TWAMP Message Exchange Categories

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

- Connection set-up 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, but 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.
    - request-session
    - start-session
    - stop-session
- 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. In addition, each packet includes an error-estimate that indicates the synchronization skew of the sender (session-sender or session-reflector) with an external time source (e.g.GPS or NTP). The packet also includes a Sequence Number.

TWAMP-Control and TWAMP-test stream support only unauthenticated security mode.

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.

Procedure

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.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ip sla responder twamp**

Example:

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

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

Step 4 **timeout** *seconds*

Example:

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

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

Step 5 **end**

Example:

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

Exits to privileged EXEC mode.

Configuration Examples for IP SLAs TWAMP Responder

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.

IP SLAs TWAMP Light

TWAMP Light is a light-weight model of TWAMP, which eliminates the need for a TWAMP control session. The test session parameters exchanged over the control session in TWAMP preconfigured at both endpoints of the TWAMP Light test session. This reduces the overhead of configuring a control session and eliminates the need for a TWAMP server that is maintained at the reflector end.

Table 4: Feature History

Feature Name	Release Information	Feature Description
TWAMP Light	Cisco IOS XE Bengaluru 17.5.1	This feature enables you to configure a TWAMP Light session using the **ip sla responder twamp-light test-session** command on the Cisco RSP2 module.

Restrictions for IP SLAs TWAMP Light

- UDP port configured on IP SLA Permanent Port cannot be configured on TWAMP Light session.
- TWAMP Light Responder and TWAMP Responder cannot be enabled simultaneously on the same UDP port.
- If a TWAMP test session is in progress, a TWAMP-Light session cannot be configured on the same port.
- If a request test session message is received from the TWAMP control client for the same port number that is used by the TWAMP Light test session, then the message will not be accepted.
- You can configure a maximum of 100 TWAMP Light sessions as allowed by the Control Plane.
- Custom DSCP values are **not** supported on TWAMP Light sessions. The DSCP value of the incoming packet is **not** used to mark the reflected packet. The default DSCP best effort value is marked in the reflected packets.

Configuring TWAMP Light

Procedure

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

Step 3	**ip sla responder twamp-light test-session** *1 local-ip 10.0.0.1 local-port 1234 remote-ip 2.2.2.2 remote-port 3456*
	Example:
	`Device(config)#ip sla responder twamp-light test-session 1 local-ip 10.0.0.1 local-port 1234 remote-ip 2.2.2.2 remote-port 3456`
	
	`Device(config)#show run | sec twamp-light`
	`ip sla responder twamp-light test-session 1`
	`local-ip 10.0.0.1 local-port 1234`
	`remote-ip 2.2.2.2 remote-port 3456`
		Configures the TWAMP Light test session on the Cisco router.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying TWAMP Light

The **show ip sla twamp-light session** command displays the TWAMP Light statistics

```
Device#show ip sla twamp-light session
Session ID: 1
Status: Active
Mode: Unauthenticated
Local Addr:10.0.0.1
Local Port: 15001
Remote Addr:1.1.1.2
Remote Port: 15002
Test packet received: 100
Test packet sent: 100
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 5357	*Two-Way Active Measurement Protocol (TWAMP)*
RFC 4656	*One-way Active Measurement Protocol (OWAMP)*

Technical Assistance

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

Feature Information for IP SLAs TWAMP Responder

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

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

Table 5: Feature Information for IP SLAs TWAMP Responder

Feature Name	Releases	Feature Information
Hardware Timestamping for IP SLA UDP Jitter Statistics	Cisco IOS XE Everest 16.6.1	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, ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M, and ASR-920-12SZ-IM).
IP SLAs TWAMP Responder on IP VRF Interface	Cisco IOS XE Release 3.18SP	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, ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M, and ASR-920-12SZ-IM).
IP SLAs TWAMP Responder v1.0	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

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 53
- Restrictions for ITU-T Y.1731 Performance Monitoring in a Service Provider Network , on page 54
- Information About ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 54
- How to Configure ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 56
- Configuration Examples for Configuring ITU-T Y.1731 Performance Monitoring Functions, on page 57
- Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network, on page 57

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

- IEEE-compliant connectivity fault management (CFM) must be configured and enabled for Y.1731 performance monitoring to function.

Note Y1731 is supported over Port Channel interfaces.

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
- Drop eligibility—marked drop ineligible
- Transmission rate

- Total interval of ETH-DM
- MEF10 frame-delay variation algorithm

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:

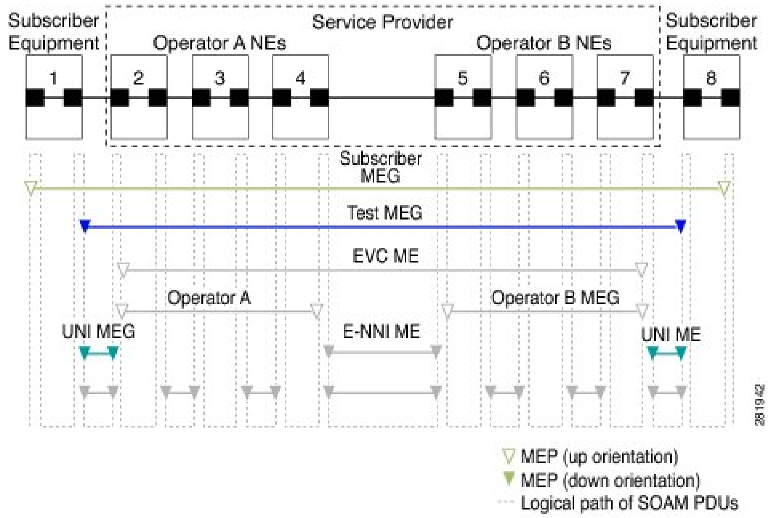
- RxTimeStampf—Time stamp of the time at which the frame with ETH-DM request information was received.
- TxTimeStampb—Time stamp of the time at which the transmitting frame with ETH-DM reply information was sent.
- The timestamping happens at the hardware level for DMM operations.

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



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 6: 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 7

Configuring an SLM

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

- Configuring SLM over VPLS, on page 59
- Restrictions for SLM support over VPLS, on page 60
- Configuring an SLM, on page 60
- Configuration Example for SLM over VPLS, on page 65

Configuring SLM over VPLS

This section describes the procedure for configuring SLM over VPLS.

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

Procedure

Step 1 Configure CFM on PE Device

For configuration details, see Configuring Ethernet Connectivity Fault Management in a Service Provider Network. In case of H-VPLS configuration, see CFM Configuration over EFP Interface with Cross Connect Feature.

Step 2 Configure CFM over VPLS using **l2 vfi** *vfi-name* **manual** *evc* command or **l2vpn vfi context** *vfi-name* command.

The evc should be the EVC name used in the CFM on PE device configuration. For configuration details, see Configuring the VFI in the PE.

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

Step 3 Configure a Sender MEP (optional task).

For configuration details, see Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation.

Restrictions for SLM support over VPLS

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

Configuring an SLM

To configure an SLM, execute the following commands:

Procedure

Step 1 **enable**

Example:

```
Router > enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal** *operation number*

—Identifies the IP SLAs' operation you want to configure.

Example:

```
Device# configure terminal
```

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.

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 **owner** *owner-id*

Example:

```
Router(config-sla-y1731-loss)# owner admin
```

(Optional) Configures the owner of an IP SLAs operation.

- *owner-id*—Specified the name of the SNMP owner. The value is from 0 to 255 ASCII characters.

Step 12 **exit**

Example:

```
Router(config-sla-y1731-loss)# exit
```

Exits IP SLA Y.1731 loss configuration mode and enters IP SLA configuration mode.

Step 13 **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*]

Example:

```
Router(config)# ip sla reaction-configuration 11 react unavailableDS
```

(Optional) Configures proactive threshold monitoring for frame loss measurements.

- *operation-number*—Identifies the IP SLAs operation for which reactions are to be configured.
- **react**—(Optional) Specifies the element to be monitored for threshold violations.
- **unavailableDS**—Specifies that a reaction should occur if the percentage of destination-to-source Frame Loss Ratio (FLR) violates the upper threshold or lower threshold.
- **unavailableSD**—Specifies that a reaction should occur if the percentage of source-to-destination FLR violates the upper threshold or lower threshold.
- **loss-ratioDS**—Specifies that a reaction should occur if the one-way destination-to-source loss-ratio violates the upper threshold or lower threshold.
- **loss-ratioSD**—Specifies that a reaction should occur if the one way source-to-destination loss-ratio violates the upper threshold or lower threshold.
- **threshold-type average**[*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 14 **ip sla logging traps**

Example:

```
Router(config)# ip sla logging traps
```

(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.

Step 15 **exit**

Example:

```
Router(config)# exit
```

Exits global configuration mode and enters privileged EXEC mode.

What to do next

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

Scheduling an IP SLA Operation

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

Procedure

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).
- **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.

Configuration Example for SLM over VPLS

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

- **sh run | i evc**

```
ethernet evcEVC_100
```

- **sh run | sec cfm**

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

- **sh run | sec 12 vfi**

```
l2 vfi VPLS-CFM manual EVC_100
vpn id 100
bridge-domain 100
neighbor 2.2.2.2 encapsulation mpls
```

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

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

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

- **sh run | sec ip sla**

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

CHAPTER 8

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 67
- Configuring DMM over VPLS, on page 67
- Configuration Example for DMM over VPLS, on page 68

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

Procedure

Step 1 Configure CFM on PE Device.

For configuration details see, Configuring Ethernet Connectivity Fault Management in a Service Provider Network .

In case of H-VPLS configuration, see, CFM Configuration over EFP Interface with Cross Connect Feature.

Step 2 Configure CFM over VPLS using **l2 vfi** *vfi-name* **manual** *evc* command or **l2vpn vfi context** *vfi-name* command.

The evc should be the EVC name used in the CFM on PE device configuration. For configuration details, see, Configuring the VFI in the PE.

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 9

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 71
- Restrictions for Smart SFP, on page 71
- Information About Loss Measurement Management (LMM), on page 72
- Configuring Loss Measurement Management, on page 76
- Configuration Examples for LMM, on page 81
- Verifying LMM, on page 81
- Additional References, on page 83
- Feature Information for Loss Measurement Management (LMM) with Smart SFP, on page 83

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 ASR 920

The following sections show the scaling numbers supported for ASR 920:

CFM, XConnect, and DMM/SLM Sessions Supported with HW Offload

Table 7: Scale Numbers (CFM and IPSLA sessions (SLM/DMM))

Feature/Parameter	ASR 920
IPSLA sessions over BD (HW offload)	300
IPSLA sessions over XConnect (HW offload)	300
IPSLA sessions over EFP (HW offload)	300
Port Channel (HW offload)	300

CFM, XConnect, and DMM/SLM Sessions Supported with SW Offload

Table 8: Scale Numbers (CFM and IPSLA sessions (SLM/DMM))

Feature/Parameter	ASR 920
IPSLA sessions over BD (SW offload)	300
IPSLA sessions over XConnect (SW offload)	300
IPSLA sessions over EFP (SW offload)	300
Port Channel (SW offload)	300

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
- Drop eligibility—marked drop ineligible
- Transmission rate
- Total interval of ETH-DM
- MEF10 frame-delay variation algorithm

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:

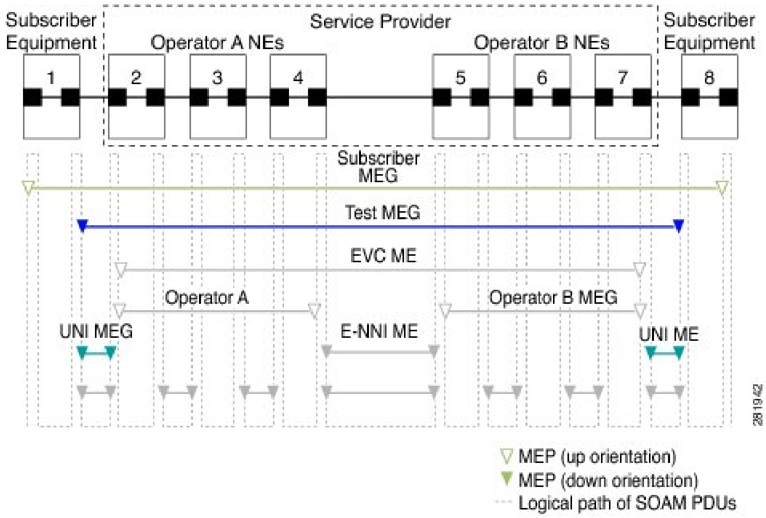
- RxTimeStampf—Time stamp of the time at which the frame with ETH-DM request information was received.
- TxTimeStampb—Time stamp of the time at which the transmitting frame with ETH-DM reply information was sent.
- The timestamping happens at the hardware level for DMM operations.

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



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

Procedure

	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.

	Command or Action	Purpose
		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.
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.

	Command or Action	Purpose
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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Device(config-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`	(Optional) Configures the length of time during which performance measurements are conducted and the results stored.

	Command or Action	Purpose
	`interval 900`	
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.
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.

	Command or Action	Purpose
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:

```
!
interface GigabitEthernet0/1/4
no ip address
negotiation auto
service instance 3 ethernet e3
encapsulation dot1q 3
service-policy input set-qos
xconnect 20.20.20.20 3 encapsulation mpls
cfm mep domain SSFP-3 mpid 3
monitor loss counter priority 1
!

!
ip sla 3
ethernet y1731 loss LMM domain SSFP-3 evc e3 mpid 30 cos 1 source mpid 3
history interval 1
aggregate interval 120
ip sla schedule 3 life 140 start-time after 00:00:05
!
```

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 9: 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 10

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.

- **Information About Service Performance Operations** , on page 85
- Restrictions for IP SLA - Service Performance Operation, on page 87
- Restrictions on the Cisco ASR 920 Routers, on page 89
- Restrictions for FPGA Based SAT, on page 92
- Information About Configuring Y.1564 to Generate and Measure Ethernet Traffic, on page 93
- Scale and Limitations for Configuring IP SLA - Service Performance Operation, on page 94
- Generating Traffic Using Y.1564, on page 96
- How to Configure IP SLA - Service Performance Testing, on page 98
- Configuration Examples for Configuring Y.1564 to Generate and Measure Ethernet Traffic , on page 116
- How to Configure Y.1564 to Generate and Measure IP Traffic , on page 120
- Configuration Examples for Configuring Y.1564 t o Generate and Measure IP Traffic , on page 135
- How to Configure IP (Layer 3) Loopback on Responder, on page 138
- SADT Overhead Accounting, on page 140
- Configurable User-Defined and EMIX Packet Size, on page 142
- SADT over VC When Access Interface is Down, on page 146
- Additional References for IP SLA - Service Performance Testing, on page 148

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 16.5.1, 10 Gigabit (10G) SAT External session is supported. Any SAT session with a rate-step greater than or equal to 1 Gbps is considered as 10G SAT session.

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 Transfer Delay (FTD) or latency—Measures the round-trip time (RTT) taken by a test frame to travel through a network device, or across the network and back to the test port.

Note If the delay is more than 4.2 sec, then the software is not capable of capturing it in SADT statistics.

- 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.
- Frame Delay Variation (FDV) or jitter—Measures the variations in the time delays between packet deliveries.

Table 10: 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.

Prerequisites for IP SLA - Service Performance Testing

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

Restrictions for IP SLA - Service Performance Operation

- SADT color aware or color blind works only if you have configured rewrite in interface EFP, else the behavior is inconsistent.

- The IP SLA sender egress and ingress VLAN should match. Ensure to configure VLAN translation in the same context.
- IP SLA classification is supported only for the DSCP/TOS marking from IP SLA command.
- One-way statistics collection is not supported.
- Layer 2 Color-Aware IP SLA is not supported for external traffic direction.
- The bridge-domain target type is not supported for external traffic direction.
- Color-Aware SLA for bridge-domain target type is not supported.
- Since SAT traffic is intrusive, any other traffic is dropped for a particular EFP.
- IPv6 address is not supported as a destination address.
- For two-way mode, the Multicast destination support is not available for IP SLA (layer 3 SLA).
- IP SLA does not support enabling a signature.
- SLA on the target with Custom Ethertype encapsulation is not supported.
- SLA on the target with 802.1ad enabled is not supported.
- Multiple active sessions are not supported on the same Ethernet EFP.
- For operations with two-way measurements, any one of the parameters, namely, port, destination MAC address, and encapsulation VLANs, should be different for SLA sessions that are simultaneously active.
- Scaling is dependent on the availability of the terminal SAT session, terminal loopback session, and egress Span session.
- For layer 2 virtual forwarding instance (VFI) or Switched Virtual Interface (SVI), only target type EFP and generator or measurement type terminal sessions should be used.
- For IMIX traffic, packet sizes of 64 bytes, 512 bytes, and 1518 bytes are supported. These packet sizes are forwarded in the ratio 7:4:1.
- For operations with layer 2 and layer 3 SLA on Trunk EFP, outer VLAN tag of the packet is mandatory.
- While a SLA session is in progress, dynamic addition of MAC access lists (ACLs) does not affect the SLA traffic.
- Priority tag SLA in external direction is supported only when the inner tag and outer tag are marked as priority tags.
- Terminal and Facility SLA sessions cannot be started on a port configured as a SPAN destination.
- Source MAC address should not be configured as multicast or broadcast MAC address.
- PIM Sparse mode is not supported for traffic generator mode and passive mode.
- SAT session fails with proper syslog messages for the following reasons:
- Only interface or service instance is supported for external session.
- VLAN or Bridge-domain service types are not supported for facility Traffic Generator and Traffic Measurement.
- EFP or Trunk EFP or bridge-domain is shut.

- The following table shows the supported egress and ingress QOS on the sender side core interface for Ethernet and IP target SLA.

Table 11: IP SLA and Type of QOS supported

IP SLA	Type of QOS	Supported on sender side core interface
IP Target SLA	Egress	Yes
IP Target SLA	Ingress	No
Ethernet Target SLA	Egress	No
Ethernet Target SLA	Ingress	Yes

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

Table 12: 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

- Service Activation layer 3 Loopback is not supported with the target interface on the router.
- Generation of burst traffic is not supported; therefore, configuration of CBS and EBS is not supported.
- IP SLAs configured with *start-time now* keyword need to be restarted after reload.
- PPS mode is *not* supported with IMIX packet size.
- For the color aware SADT to work as expected, rewrite EFP should be present.

Restrictions on the Cisco ASR 920 Routers

- SADT Internal sessions are not supported on ASIC interface on the RSP2 module.

  During interoperability of SADT with ME3600 and ASR920 routers, you experience a loss in ASR920 loopback with IMIX traffic. It is the expected behavior as the traffic is more bursty on ME3600.

- Only DSCP-based marking is supported for IP Target operations.
- The session duration is limited to multiples of 10; user input is rounded down to the nearest multiple of 10.
- Quality of Service (QOS) on any target type with IP SLA is not supported on layer 2 and layer 3 routers.
- Layer 3 IP SLA is not supported on external traffic direction.
- Layer 3 SLA Loopback is not supported for labelled incoming packets.
- For layer 3 Loopback, if the target type is service instance, the core and access side EFP should have the same encapsulation.
- For layer 3 Loopback, if the target type is VRF, only encapsulation untagged is supported. The loopback session is not supported for the VRF target types even for same encapsulation on access and core EFPs.
- For layer 3 Loopback, if the target type is bridge domain, only encapsulation untagged is supported. The loopback session is not supported for the bridge domain target types, even for the same encapsulation on access and core EFPs.
- For operations with passive measurement mode and target type EFP, the same destination MAC address cannot be used for any other traffic on a port as the loopback MAC Address Tables (CAM) tables contain the channel numbers and the destination MAC address. As a result, multiple SLAs with the same destination MAC address, on the same port active at the same time, are not supported for passive measurement mode.
- For operations with EFP using XConnect, only the target type EFP and terminal sessions for Tx and Rx statistics are supported.
- For layer 2 internal sessions with Rx statistics, either only four non-color-aware sessions, or one color-aware session and one non-color-aware session are supported.
- Port channel is not supported.
- For operations with SLA in PPS mode, an additional packet is forwarded.
- The minimum supported value for rate step is 1024 pps.
- While running SADT, the packet that matches the SLA profile source MAC, VLAN or untagged, is counted in the RX. For example, if you schedule an SLA and start PING in the same time frame, PING fails, since the ping acknowledgement packet is accounted in SLA RX packet. Similarly, the LL discovery packet from the responder is accounted in SLA RX. So, there is one extra packet and the same packet is not accounted in the LL discovery counter.

Restrictions for 10G SAT

- The IP SLA packets are generated and forwarded in ratio of 1:1:1:1:1 from UNI or NNI port based on your configuration.
- 10G service activation test (SAT) is supported only for Layer 2 traffic in external and internal direction.
- 10G SAT is not supported in internal direction for releases prior to 16.12.x.
- Only color blind configurations are supported. CIR, EIR, and other color aware parameters is not supported.
- 10G SAT can only run in two-way mode.

- Effective from Cisco IOS XE Gibraltar 16.12.1, Delay, and Jitter measurements are supported.
- 10G SAT target type that is supported is only on access EFP.
- A combination of 1G and 10G SAT sessions cannot be run in parallel.
- At SLA run time, SAT statistics may not match. Statistics must be validated only after SLA completes. While SAT SLA is running, there might be instances where Rx might be greater than Tx. This is because of slow retrieval of statistics from the hardware. Statistics should be verified only after SAT operation is complete.
- Layer 3 packets for Layer 2 facility SAT 10G session is not supported.
- Only Layer 2 related parameters (SRC, MAC, VLAN, COS) should be configured while constructing the packet profile.
- Ethertype of IPv4 or IPv6 is not supported.
- Layer 3 packet headers should not be used in profile packet.
- Multiple rate-steps that are mentioned in a single command can only be mentioned in incremental order.
- With 10G SAT running in external mode, while QoS egress shaper policy is applied on the same SAT interface, SAT traffic generation is being affected based on the shaper value. SAT rate-step is adjusted by shaper policy. However, when policer based policy is applied inbound, there is no impact with regards to SAT traffic being policed. Despite the policer value configured, no policing happens for the return traffic on SAT interface. This is due to the configured internal ACL to handle the SAT statistics.
- If a 10G SAT session is running (with a rate-step greater than or equal to 1 Gbps), a second 1G or 10G SAT session should not be executed parallely.
- The SAT rate-step upper limits should be defined in such a way that BFD has some bandwidth for itself and ensures that the OSPF flaps do not occur. The upper limit for FPGA traffic generation for SAT is same in both SAT 1G and 10G. So, the upper limit of SAT 1G x 10 are applicable for SAT 10G to avoid the OSPF flaps.
- OIR and SSO are not supported with SAT. SLA is to be stopped and re-started manually after these triggers.
- SADT session and Ethernet loopback (ELB) on the same service instance of an interface is not supported.
- 10G SAT with 802.1ad is not supported.
- A delay of 10 seconds is recommended between two 10G SAT iterations or between two SLA runs (serial run).
- A combination of untagged and default should never be configured on an interface for launching 10G SLA session. 10G SAT on encapsulation default does not work when encapsulation untagged is configured on the interface.
- Even with 10G SAT, maximum FPGA available for 920 is 1G. 10G SAT rate is achieved by generating the packets in FPGA (upto 1 Gbps) and multiplying it by 10 on the hardware. Hence, a maximum of 1G FPGA is only available for all processes including BFD, SAT, NetFlow, and so on So, crossing the 1G cumulative threshold in FPGA causes flaps on the various interfaces that involve FPGA.
- 10G SAT is not supported over VRF and Port-Channel interfaces.
- SADT 10G session uses a shadow session with given MAC + 1 (0011.1111.2222 to 0011.1111.2223).

- 10G SADT internal is supports only Xconnect EFP and Plain EFP.
- 10G SADT is not supported on L2VFI (Virtual Forwarding Interface) and local connect.
- 10G SADT Color-aware configurations are not supported.

Note

- Overall throughput in the system slightly varies up to +/- 2% from the mentioned rate-step value.
- Color-aware case "rewrite ingress tag pop 1 symmetric" is mandatory under the efp configuration.

Restrictions for SAT Two-Way Sessions on EFP Xconnect on the Cisco ASR 920 Routers

- For operations with EFP using XConnect, the rewrite ingress tag pop 1 symmetric command is not supported for two-way sessions when Class of Service (COS) value is a part of the packet profile.
- For operations with EFP using XConnect, the rewrite command is not supported when Class of Service (COS) value is configured for the SLA.
- For EVC with XConnect targets, CoS marking based on color for the color-aware cases is performed on the outer layer 2 header VLAN tags (if applicable). As a result, this marking should be retained across the network so that it is available on the packet, which is received at the remote end (passive measurement mode) or the same end after loopback at the remote end (two-way mode). If this CoS marking is not retained, there is no way identifying the color of the different packets and perform color-aware measurement.
- Color-aware two-way sessions measurement is not supported for the restrictions listed above.

Restrictions for FPGA Based SAT

The following restrictions ae applicable only on the Cisco ASR-920-12SZ-A, Cisco ASR-920-12SZ-D, Cisco ASR-920-12SZ-IM, and Cisco ASR-920U-12SZ-IM variants of the Cisco ASR 920 router:

- For two-way sessions, source MAC address (last 2 bytes) of configured IP SLA sessions should be unique.
- For passive measurement sessions, destination MAC address (last 2 bytes) of configured IP SLA sessions should be unique.
- PPS may not match exactly.
- FPGA supports a minimum of 16 Kbps and a maximum of 10 Gbps. FPGA cannot generate traffic with 100 percent accuracy. There may be a little difference between configured bandwidth and actual bandwidth.
- For external direction SADT session, Rx and Tx packet count are same but Rx bytes and Tx bytes may not match exactly if the target EFP is configured with a rewrite action.
- In some scenarios, SLA statistics collection is delayed by 1 second. This may impact the overall throughput.
- Color aware statistics do not work if BDI is present for the bridge domain.
- Dynamic modification is not supported while the session is running.

- VLAN should be configured at the target interface in the SLA session. If the VLAN is not part of the interface configuration, packets are not handled properly.
- If the outer VLAN is not specified but the inner VLAN is specified for the target EFP, by default the outer VLAN is 4095, the outer COS is 7, and the CFI is 1. If both the outer and the inner VLAN is not specified, the VLAN tags are fetched from the EFP.
- The outer VLAN is required for the target TEFP.
- SADT supports only two rate three color policy.

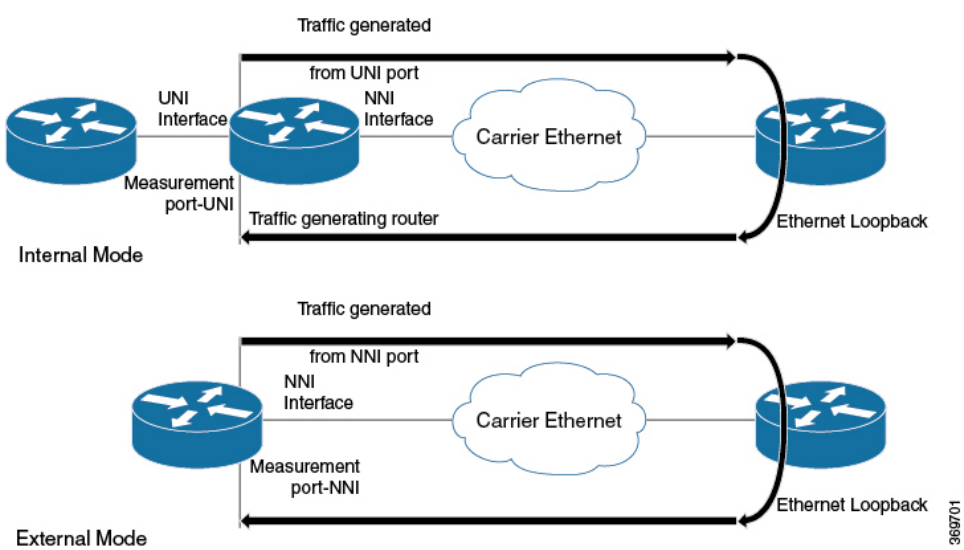
Information About Configuring Y.1564 to Generate and Measure Ethernet Traffic

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.

Figure 8: Traffic Generator Topology



The following table provides details of the different service types and traffic directions supported for each service type.

Table 13: Service Types and Their Corresponding Traffic Direction for IP Target SLA

Service Type	Traffic Direction for IP Target SLA
Service Instance	Internal
Interface (Physical)	Internal
Bridge Domain	Internal
VRF	Internal

Table 14: Service Types and Their Corresponding Traffic Direction for Ethernet Target SLA

Service Type	Traffic Direction for Ethernet Target SLA
Service Instance	Internal and External
Bridge Domain	Internal

Scale and Limitations for Configuring IP SLA - Service Performance Operation

The following table shows the scaling numbers supported for different SAT sessions.

Table 15: Scaling Numbers for IP SLA

IP SLA	1G Scaling Numbers Supported	10G Scaling Numbers (Internal /External) Supported
IP Target Color Aware SLA	5	NA NA
IP Target Color Blind SLA	15	1 NA
Ethernet Target Color-Aware SLA	1	NA NA
Ethernet Target Color Blind SLA	8 (4 Internal SLA + 4 External SLA)	1 1
IP Target Loopback SLA	4	1 NA

Note The scale limit with the combination of Color-Aware and Color Blind IP SLA depends on the number of TCAM entries that the combination of SAT sessions consume. The Color-Aware session takes 3 entries for each session and the Color Blind consumes 1 entry for each session. Hence, the maximum scale for Color-Aware sessions is 15 (3 * 5 = 15 entries) and that for the Color Blind sessions is 15 (15 * 1 = 15 entries). Combination of Color-Aware and Color Blind depends on the number of TCAM entries consumed by the SAT profile and it is limited to entries.

Note If a 10G SADT session is running then no other 1G or 10G session can be started.

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

Table 16: Throughput Measurement for Each Packet Size

Packet Size (Bytes)	1G Max Rate (kbps)	10G Max Rate (kbps)
64	469848	4698480
128	638061	6380610
256	775123	7751230
512	867758	8677580
1024	922728	9227280
1280	934554	9345540
1518	942124	9421240
9216	977675	9776750
IMIX	788000	7880000

Note The Max Rate mentioned in the table above is the maximum SLA rate supported by router and it is independent of SLA sessions. Max Rate can be achieved in a single SLA session or combination of two or more SLA sessions. Exceeding the supported Max Rate might impact other services.

Note With a given frequency time configuration, SLA will run for duration time configured on the SLA and restart after the delay time. It will continue to get into a loop until the life time configuration. To calculate delay time use delay time = frequency time - duration time.

Generating Traffic Using Y.1564

Follow these steps to generate traffic using Y.1564:

Procedure

	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.
	`Device(config)# ip sla 100`
	`Device(config-ip-sla)#`
	`service-performance type ethernet`
	`dest-mac-addr 0001.0002.0003 interface`
	`TenGigabitEthernet0/0/4 service instance`
	` 100`
	`Device(config-ip-sla-service-performance)#`
	` aggregation interval buckets 2`
	`Device(config-ip-sla-service-performance)#`
	` frequency iteration 2 delay 10`
	`Device(config-ip-sla-service-performance)#`
	` profile packet`
	`Device(config-sla-service-performance-packet)#`
	` packet-size 256`
	`Device(config-sla-service-performance-packet)#`
	` outer-vlan 100`
	`Device(config-sla-service-performance-packet)#`
	` profile traffic direction external`
	`Device(config-sla-service-performance-traffic)#`
	` rate-step kbps 1000`
	`Device(config-ip-sla-service-performance)#`
	` end`
	`Device #`	

Step 3	Configure Ethernet Loopback at the remote end.	For information on Ethernet Loopback, see "Understanding Ethernet Loopback" section in the *Layer 2 Configuration Guide, Cisco IOS XE Release* .
Step 4	Configure loopback on SAT IP SLA configuration itself at the remote end. **Example:** `ip sla 1`	

	Command or Action	Purpose

	` 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 5	Start the IP SLA session: **Example:** `Router(config)# ip sla schedule [sla_id] start-time [hh:mm | hh:mm:ss | now | pending | random]`	**Note** Due to packet overhead (64-byte packets), a total of only 469 Mbit/sec of traffic is supported at a time. This bandwidth is shared by all active sessions. This is applicable only for Cisco RSP2 module. For more information, see Table 4.

Note Whenever the rate-step is set as line rate (1 Gbps) in case of 1G link, you will see the FLR % as non-zero. In such case, reduce the rate-step to less than the line rate to attain 0% FLR.

How to Configure IP SLA - Service Performance Testing

Y.1564 support on dot1ad Encapsulation

Table 17: 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.

Procedure

	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.

	Command or Action	Purpose
Step 4	**service-performance type ethernet dest-mac-addr** *dest-mac* { **service instance | bridge**} **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 are: • service instance • bridge Only service instance is supported as target-type on 10G SAT.
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 | loss | no | throughput | receive | delay | jitter** **Example:** `Device(config-ip-sla-service-performance-measurement)# throughput`	Specifies the measurement type based on the service performance is calculated. The options are: • **default** - Sets a command to its defaults. • **loss** - Specifies the measurement, such as frame loss.

	Command or Action	Purpose
		• **throughput** - Specifies the measurement such as average rate of successful frame delivery. • **receive** - Specifies the passive measurement mode. • **delay** - Specifies the measurement that is frame delay (FTD). This is not supported on 10G. • **jitter** - Specifies the measurement that is frame delay variation (FDV). This is not supported on 10G.
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, 9216 bytes, and IMIX. • **src-mac-addr** - Specifies the source MAC address in H.H.H format.

	Command or Action	Purpose
		• **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.
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. Only external profile traffic direction is supported for 10G. **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.

Configuring Ethernet Target Color-Aware Traffic Generation

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

Procedure

	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-addr* {**bridge-domain** *domain_id* | **interface** *interface* [**service instance** *efp-id*]} **Example:** `Device(config-ip-sla))#service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitEthernet0/0/10 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 option is: • service instance
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iteration.
Step 6	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.
Step 7	**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 8	**default** | **exit** | **inner-cos** | **inner-vlan** | **no** | **outer-cos** | **outer-vlan** | **packet-size** | **src-mac-addr** | **outer-eth-type** | **inner-eth-type**	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

	Command or Action	Purpose
	Example: `Device(config-ip-sla-service-performance-packet)#src-mac-addr 4055.3989.7b56`	the interface from which the message is sent. • **inner-vlan** - Specifies the VLAN ID for the inner vlan tag of the interface from which the message is sent. • **outer-cos** - Specifies the CoS value that is populated in the outer VLAN tag of the packet. • **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **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.
Step 9	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the profile packet mode.
Step 10	**profile traffic direction** [**internal** | **external**] **cir** *number* or **eir** *number* or **cbs** *number* or **ebs** *number* or **conform-color set-cos-transmit** *cos_value* or **exceed-color set-cos-transmit** *cos_value* or **default** or **exit** or **no** or **rate step kbps | pps** *number*	Defines an upper limit on the volume of the expected service frames belonging to a particular service instance. If a Traffic profile is not specified, the Service Performance probe is in passive measurement mode.

	Command or Action	Purpose

	Example:
	`Device(config-ip-sla-service-performance)# profile traffic direction internal`
	`Device(config-ip-sla-service-performance-traffic)# cir 45000`
	`Device(config-ip-sla-service-performance-traffic)# eir 45000`
	`Device(config-ip-sla-service-performance-traffic)# conform-color set-cos-transmit 4`
	`Device(config-ip-sla-service-performance-traffic)# exceed-color set-cos-transmit 5`
	`Device(config-ip-sla-service-performance-traffic)# rate-step kbps 5000 9000`
		• **cir** - Committed Information Rate.
		• **cbs** - Committed Burst Size.
		• **conform-color** - Sets the color conform.
		Note **coform-color** and **exceed-color** keywords are available only when **cir** or **eir** is configured.
		• **default** - Sets a command to its defaults.
		• **drop** - Drops the packet.
		• **eir** - Excess Information Rate.
		• **ebs** - Excess Burst Size.
		• **exceed-color** - Sets the color-exceed.
		• **exit** - Exits the traffic mode.
		• **no** - Negates a command or sets its defaults.
		• **set-cos-transmit** *cos_value* - Sets the CoS value to a new value and sends the packet. The valid range is from 0 to 7.
		• **transmit** - Sends the packet without altering it. This is the default value.
		• **default** - Sets a command to its defaults.
		• **rate step kbps** - Specifies the transmission rate in kbps. The rate-step range is from 1 to 1000000 (1 Kbps to 1 Gbps).
		• **rate step pps** - Specifies the transmission rate in pps. The rate-step range is from 1 to 1000000.
		Note The command **rate-step kbps | pps number** is mandatory for traffic generation.

Example

```
Device(config-ip-sla-service-performance)#profile packet
Device(config-ip-sla-service-performance-packet)#outer-vlan 100
Device(config-ip-sla-service-performance-packet)#outer-cos 5
```

```
Device(config-ip-sla-service-performance-packet)#exit
Device(config-ip-sla-service-performance)#profile traffic direction internal
Device(config-ip-sla-service-performance-traffi c)# cir 45000
Device(config-ip-sla-service-performance-traffi c)# eir 45000
Device(config-ip-sla-service-performance-traffic)# conform-color set-cos-transmit 4
Device(config-ip-sla-service-performance-traffic)# exceed-color set-cos-transmit 5
Device(config-ip-sla-service-performance-traffic)# rate-step kbps 1000
Device(config-ip-sla)# duration time 15
Device(config-ip-sla)# frequency iteration 4 delay 1
```

Configuring Ethernet Target Two-Way Color-Aware Session

Perform the following steps to configure ethernet target two-way color-aware session.

Note The default **frequency iteration** command value may cause the duration command to be rejected for higher values. In this case, the **frequency iteration** command is recommended before the execution of **duration** command.

Procedure

	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-addr* |**interface** *interface* [**service instance** *efp-id*] **Example:** `Device(config-ip-sla))#service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitEthernet0/0/10 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 are: • service instance • bridge
Step 5	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.

	Command or Action	Purpose
Step 6	**profile packet** **Example:** `Device(config-ip-sla-service-performance)# profile packet`	Specifies the packet profile. A packet profile defines the packets to be generated. It also defines the filter for incoming packets to be measured.
Step 7	**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 is sent. • **inner-vlan** - Specifies the VLAN ID for the inner vlan tag of the interface from which the message is sent. • **outer-cos** - Specifies the CoS value that is populated in the outer VLAN tag of the packet. • **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **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 8	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the profile packet mode.

Step 9	**profile traffic direction** [**internal** |**external**] **cir** *number* or **eir** *number* or **cbs** *number* or **ebs** *number* or **conform-color set-cos-transmit** *cos_value* or **exceed-color set-cos-transmit** *cos_value* or **default** or **exit** or **no** or **rate step kbps | pps** *number*
	Example:
	`Device(config-ip-sla-service-performance)# profile traffic direction internal`
	`Device(config-ip-sla-service-performance-traffic)# cir 45000`
	`Device(config-ip-sla-service-performance-traffic)# eir 45000`
	`Device(config-ip-sla-service-performance-traffic)# conform-color set-cos-transmit 4`
	`Device(config-ip-sla-service-performance-traffic)# exceed-color set-cos-transmit 5`
	`Device(config-ip-sla-service-performance-traffic)# rate-step kbps 1000`
		Specifies the in-line traffic profile or enables the selection of a preconfigured traffic profile. A traffic profile defines an upper limit on the volume of the expected service frames belonging to a particular service instance. If a Traffic profile is not specified, the Service Performance probe is in passive measurement mode.
		• **cir** - Committed Information Rate.
		• **cbs** - Committed Burst Size.
		• **conform-color** - Sets the color conform.
		• **default** - Sets a command to its defaults.
		• **drop** - Drops the packet.
		• **eir** - Excess Information Rate.
		• **ebs** - Excess Burst Size.
		• **exceed-color** - Sets the color-exceed.
		• **exit** - Exits the traffic mode.
		• **no** - Negates a command or sets its defaults.
		• **set-cos-transmit** *cos_value* - Sets the CoS value to a new value and sends the packet. The valid range is from 0 to 7.
		• **transmit** - Sends the packet without altering it. This is the default value.
		Note This command is required to configure the **rate step kbps** command.
		• **default** - Sets a command to its defaults.
		• **rate step kbps** - Specifies the transmission rate in kbps. The rate-step range is from 1 to 1000000 (1 Kbps to 1 Gbps).

	Command or Action	Purpose
		Note The command **rate-step kbps | pps number** is mandatory for traffic generation.
Step 10	**measurement-type direction** [**internal** |**external**] **conform-color cos** *cos_value* **exceed-color cos** *cos value* **Example:** `Device(config-ip-sla)# measurement-type direction internal cos 7`	Specifies the direction of measurement.
Step 11	**default** | **exit** | **loss** | **throughput** | **receive** | **delay** | **jitter** **Example:** `Device(config-ip-sla-service-performance-measurement)# throughput`	Specifies the measurement type based on which the service performance is calculated. The options are: • **default**: Sets a command to its defaults. • **loss**: Specifies the measurement such as frame loss. • **throughput**: Specifies the measurement such as average rate of successful frame delivery. • **receive**: Specifies the passive measurement mode. • **delay** - Specifies the measurement that is frame delay (FTD). • **jitter** - Specifies the measurement that is frame delay variation (FDV).
Step 12	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iterations.

Example

```
ip sla 3
service-performance type ether des
0033.3333.3333 interface gig 0/0/3
service instance 1
profile packet
outer-vlan 100
outer-cos 5
packet-size 128
ethertype ipv4
exit
```

```
profile traffic direction internal
cir 45000
eir 45000
cbs 45000
ebs 45000
conform-color set-cos-transmit 7
exceed-color set-cos-transmit 5
rate-step kbps 30000 45000 65000
90000
exit
measurement-type direction internal
conform-color cos 7
exceed-color cos 5
receive
throughput
loss
delay
jitter
duration time 20
frequency iteration 1 delay 2
```

Configuring Ethernet Target Passive Color-Aware Measurement

Perform the following steps to configure ethernet target passive color-aware measurement.

Procedure

	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_addr* {**bridge-domain** *domain_id* | **interface** *interface* [**service instance** *efp-id*]} **Example:** `Device(config-ip-sla))#service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitEthernet0/0/10 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 are: • service instance • bridge

	Command or Action	Purpose
Step 5	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.
Step 6	**profile packet** **Example:** `Device(config-ip-sla-service-performance)# profile packet`	Specifies the packet profile. A packet profile defines the filter for incoming packets to be measured.
Step 7	**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 is sent. • **inner-vlan** - Specifies the VLAN ID for the inner vlan tag of the interface from which the message is sent. • **outer-cos** - Specifies the CoS value that is populated in the outer VLAN tag of the packet. • **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **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.

	Command or Action	Purpose
		Note If you do not specify the encapsulation type in the packet profile, `dot1q` is used by default.
Step 8	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the profile packet mode.
Step 9	**measurement-type direction** [**internal** |**external**] **conforn-color cos** *cos_value* **exceed-color cos** *cos_value* **Example:** `Device(config-ip-sla)# measurement-type direction internal cos 7`	Specifies the direction of measurement.
Step 10	**default** | **exit** | **loss** | **throughput** | **receive** **Example:** `Device(config-ip-sla-service-performance-measurement)# throughput`	Specifies the measurement type based on which the service performance is calculated. The options are: • **default** - Sets a command to its defaults. • **loss** - Specifies the measurement such as frame loss. • **throughput** - Specifies the measurement such as average rate of successful frame delivery. • **receive** - Specifies the passive measurement mode.
Step 11	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iterations.

Example

```
ip sla 3
service-performance type ether des
0033.3333.3333 interface gig 0/0/3
service instance 1
profile packet
outer-vlan 100
outer-cos 5
packet-size 128
ethertype ipv4
exit
measure direction internal
conform-color cos 7
exceed-color cos 5
```

```
receive
throughput
loss
duration time 20
frequency iteration 1 delay 2
```

Configuring Ethernet Target for Color-Aware Traffic Generation with IMIX

Perform the following steps to configure ethernet target for color-aware traffic generation with IMIX.

Procedure

	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_addr* {**bridge-domain** *domain_id* | **interface** *interface* [**service instance** *efp-id*]} **Example:** `Device(config-ip-sla))#service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitEthernet0/0/10 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 are: • service instance • bridge
Step 5	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.
Step 6	**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 7	**default** | **exit** | **inner-cos** | **inner-vlan** | **no** | **outer-cos** | **outer-vlan** | **packet-size imix** | **src-mac-addr** | **outer-eth-type** | **inner-eth-type**	Specifies the packet type. The options are: • **default** - Sets a command to its defaults.

	Command or Action	Purpose
	Example: `Device(config-ip-sla-service-performance-packet)#packet-size imix`	• **inner-cos** - Specifies the class of service (CoS) value for the inner VLAN tag of the interface from which the message is sent. • **inner-vlan** - Specifies the VLAN ID for the inner vlan tag of the interface from which the message is sent. • **outer-cos** - Specifies the CoS value that is populated in the outer VLAN tag of the packet. • **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **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** For IMIX, the packet-size should be explicitly mentioned as IMIX. **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.
Step 8	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the profile packet mode.

	Command or Action	Purpose

Step 9	**profile packet direction** [**internal** | **external**] **cir** *number* or **eir** *number* or **cbs** *number* or **ebs** *number* or **conform-color set-cos-transmit** *cos_value* or **exceed-color set-cos-transmit** *cos_value* or **default** or **exit** or **no** or **rate step kbps**
	Example:
	`Device(config-ip-sla-service-performance)# profile traffic direction internal`
	`Device(config-ip-sla-service-performance-traffic)# cir 45000`
	`Device(config-ip-sla-service-performance-traffic)# eir 45000`
	`Device(config-ip-sla-service-performance-traffic)# cbs 45000`
	`Device(config-ip-sla-service-performance-traffic)# ebs 45000`
	`Device(config-ip-sla-service-performance-traffic)# conform-color set-cos-transmit 4`
	`Device(config-ip-sla-service-performance-traffic)# exceed-color set-cos-transmit 5`
	`Device(config-ip-sla-service-performance-traffic)# rate-step kbps 1000`
		Specifies the in-line traffic profile or enables the selection of a pre-configured traffic profile. A traffic profile defines an upper limit on the volume of the expected service frames belonging to a particular service instance. If a traffic profile is not specified, the Service Performance probe is in passive measurement mode.
		• **cir** - It is the Committed Information Rate.
		• **cbs** - It is the Committed Burst Size.
		• **conform-color** - Sets the conform color.
		• **default** - Sets a command to its defaults.
		• **drop** - Drops the packet.
		• **eir** - It is the Excess Information rate.
		• **ebs** - It is the Excess Burst Size.
		• **exceed-color** - Sets the exceed color.
		• **exit** - Exits the traffic mode.
		• **no** - Negates a command or sets its defaults.
		• **rate step kbps** - Sets the rate step.
		• **set-cos-transmit** *cos_value* - Sets the CoS value to a new value, and sends the packet. The valid range is from 0 to 7.
		• **transmit** - Sends the packet without altering it. This is the default value.
		• **default** - Sets a command to its defaults.
		Note This command is required to configure the **rate step kbps** command.

Step 10	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iterations.

Example

```
ip sla 3
service-performance type ether des 0033.3333.3333 interface gig 0/0/3
service instance 1
profile packet
outer-vlan 100
outer-cos 5
packet-size mix
ethertype ipv4
exit
profile traffic direction internal
cir 45000
eir 45000
cbs 45000
ebs 45000
conform-color set-cos-transmit 7
exceed-color set-cos-transmit 5
rate-step kbps 30000 45000 65000
90000
exit
duration time 20
frequency iteration 1 delay 2
```

Configuring Y.1564 Traffic payload pattern

Perform the following steps to configure Y.1564 Traffic payload pattern.

Procedure

	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-addr* |**interface** *interface* [**service instance** *efp-id*] **Example:** `Device(config-ip-sla))#service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitEthernet0/0/10 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 are: • Service instance • Bridge

	Command or Action	Purpose
Step 5	**signature** 45] **Example:** `Device(config-ip-sla-service-performance)#signature 45`	Specifies the payload pattern for Y.1564 traffic.
Step 6	**exit** **Example:** `Device(config-ip-sla-service-performance)#exit`	Exits mode.

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

This section shows sample configurations for traffic generation.

Example: Traffic Generation — Target Service Instance

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

```
ip sla 100
service-performance type ethernet dest-mac-addr 0001.0002.0003 interface
TenGigabitEthernet0/0/4 service instance 100
profile packet
packet-size 256
outer-vlan 100
profile traffic direction internal
rate-step kbps 1000
aggregation interval buckets 2
frequency iteration 2 delay 10
end
```

Example: Traffic Generation — Target Bridge Domain

This section shows sample configuration for traffic generation – target bridge domain.

```
ip sla 100
service-performance type ethernet dest-mac-addr 0001.0002.0003 bridge-domain 100
profile packet
packet-size 256
outer-vlan 100
aggregation interval buckets 2
frequency iteration 2 delay 10
end
```

Example: Two-Way Session—Target Service Instance

The following is a sample configuration for a two-way measurement session of service instance internal target type.

```
ip sla 100
service-performance type ethernet dest-mac-addr 0001.0002.0003 interface
TenGigabitEthernet0/0/2 service instance 100
measurement-type direction internal
loss
throughput

delay
jitter
profile packet
packet-size 64
outer-vlan 100
inner-vlan 200
profile traffic direction internal
rate-step kbps 1000
aggregation interval buckets 2
frequency iteration 2 delay 10
end
```

Example: Two-Way Session — Target Bridge Domain

The following is a sample configuration for a two-way internal measurement and generation session with target type Bridge Domain.

```
ip sla 100
service-performance type ethernet dest-mac-addr 0001.0002.0003 bridge-domain 100
measurement-type direction internal
loss
throughput
delay
jitter
profile packet
packet-size 64
outer-vlan 100
inner-vlan 200
profile traffic direction internal
rate-step kbps 1000
aggregation interval buckets 2
frequency iteration 2 delay 10
end
```

Example: Passive Measurement Mode — Target Service Instance

The following is a sample configuration for passive measurement session for target service instance.

```
ip sla 100
service-performance type ethernet dest-mac-addr 0001.0002.0003 interface
TenGigabitEthernet0/0/4 service instance 100
measurement-type direction internal
loss
throughput
aggregation interval buckets 2
frequency iteration 2 delay 10
end
```

Example: Passive Measurement Mode — Target Bridge Domain

The following is a sample configuration for passive measurement session for bridge domain target.

```
ip sla 100
service-performance type ethernet dest-mac-addr 0001.0002.0003 bridge-domain 100
measurement-type direction internal
loss
throughput
aggregation interval buckets 2
frequency iteration 2 delay 10
end
```

Example: Traffic Generation Mode — Color Aware

The following is a sample output for traffic generation mode—color aware.

```
ip sla 3
service-performance type ether des 0033.3333.3333 int gig 0/0/7 service instance 1
 profile packet
outer-vlan 100
outer-cos 5 packet-size 128 ethertype ipv4 exit
profile traffic dir int cir 45000
eir 45000
 cbs 45000
ebs 45000
conform-color set-cos-transmit 7 exceed-color set-cos-transmit 5
rate-step kbps 30000 45000 65000 90000 exit
duration time 20
frequency iteration 1 delay 2
```

Example: Traffic Generation Mode with IMIX — Color Aware

The following is a sample output for traffic generation mode with IMIX — color aware.

```
ip sla 3
service-performance type ether des 0033.3333.3333 int gig 0/0/7 service instance 1
 profile packet
outer-vlan 100 outer-cos 5 packet-size imix ethertype ipv4 exit
profile traffic dir int
cir 45000 eir 45000
 cbs 45000
ebs 45000
conform-color set-cos-transmit 7
exceed-color set-cos-transmit 5
rate-step kbps 30000 45000 65000 90000 exit
duration time 20
frequency iteration 1 delay 2
```

Example: Two-way Color-Aware Measurement Session

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

```
ip sla 3
service-performance type ether des 0033.3333.3333 int gig 0/0/7 service instance 1
 profile packet
outer-vlan 100
```

```
outer-cos 5 packet-size 128 ethertype ipv4 exit
profile traffic dir int cir 45000
eir 45000
 cbs 45000
ebs 45000
conform-color set-cos-transmit 7 exceed-color set-cos-transmit 5
rate-step kbps 30000 45000 65000 90000 exit
measure dir internal conform-color cos 7 exceed-color cos 5 receive
throughput loss delay jitter
duration time 20
frequency iteration 1 delay 2
```

Example: Passive Color-Aware Measurement Session

The following is a sample configuration for a passive color-aware measurement session.

```
ip sla 3
service-performance type ether des 0033.3333.3333 int gig 0/0/7 service instance 1
 profile packet
outer-vlan 100 outer-cos 5 packet-size 128 ethertype ipv4 exit
measure dir internal conform-color cos 7 exceed-color cos 5 receive
throughput
loss
duration time 20
frequency iteration 1 delay 2
```

Example: Two-Way Session

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

```
show ip sla statistics 12345

IPSLAs Latest Operation Statistics

IPSLA operation id: 12345
Type of operation: Ethernet Service Performance
Test mode: Two-way Measurement
Steps Tested (kbps): 10000 20000 25000
Test duration: 20 seconds

Latest measurement:  *15:54:44.007 IST Mon May 18 2015
Latest return code:  Oper End of Life

Overall Throughput: 24850 kbps

Step 1 (10000 kbps):
Stats:
IR(kbps) FL   FLR      Avail              FTD Min/Avg/Max      FDV Min/Avg/Max
9944      0     0.00%  100.00%  41.44us/46.06us/77.68us  0ns/12.08us/34.52us
Tx Packets: 16377 Tx Bytes: 24860286
Rx Packets: 16377 Rx Bytes: 24860286
Step Duration: 20 seconds
```

Example: 10G Ethernet Two-Way Color Blind Session

The following is a sample configuration for a 10G ethernet two-way color blind session:

```
router#show run | sec ip sla 200
ip sla 200
service-performance type ethernet dest-mac-addr 0000.0000.2200 interface
TenGigabitEthernet0/0/2 service instance 200
  frequency iteration 2 delay 10
  aggregation interval buckets 2
  measurement-type direction external
   loss
   receive
   throughput
  profile packet
   outer-cos 2
   outer-vlan 200
   packet-size 1024
   src-mac-addr 0000.0000.4400
  profile traffic direction external
   rate-step kbps 9000000
  duration time 60
```

The following is the sample output for the 10G ethernet two-way color blind session:

```
router#show ip sla statistics 200
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
Type of operation: Ethernet Service Performance
Test mode: Two-way Measurement
Steps Tested (kbps): 9000000
Test duration: 60 seconds

Latest measurement:  *18:04:34.975 IST Wed Mar 29 2017
Latest return code:  Oper End of Life

Overall Throughput: 8943460 kbps

Step 1 (9000000 kbps):
Stats:
IR(kbps)  FL          FLR      Avail
8943460   0           0.00%    100.00%
Tx Packets: 65503860  Tx Bytes: 67075952640
Rx Packets: 65503860  Rx Bytes: 67075952640
Step Duration: 60 seconds
```

How to Configure Y.1564 to Generate and Measure IP Traffic

This section shows how to configure Y.1564 to generate and measure IP traffic.

Effective Cisco IOS XE Release 3.16, the following features are supported on the routers:

- IP flow parameters (DA/SA) Generation
- IP flow parameters (DA/SA) Measurement
- Color-Blind IP flow Generation and Measurement
- Color-Aware IP flow Generation: Differentiated services code point (DSCP) based
- Color-Aware IP flow Measurement: DSCP based
- IMIX Traffic Generation type (combination of 64, 512, and 1518 byte packets)

Note For vrf targets, the vrf-id specified in the SLA configuration should be the VRF Id derived from the output of the show vrf detail | include VRF Id STR

```
#sh vrf det | i VRF Id
VRF Mgmt-intf (VRF Id = 1); default RD <not set>; default VPNID <not set>
VRF SAT (VRF Id = 2); default RD 100:1; default VPNID <not set>
```

Configuring IP Target Color-Aware Traffic Generation

Perform the following steps to configure IP target color-aware traffic generation.

Note The **default frequency iteration** command value may cause the duration command to be rejected for higher values. In this case, the **frequency iteration** command is recommended before the execution of the **duration** command.

Note Configuring **source-ip-addr** is mandatory for layer 3 IP SLA.

Procedure

	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 ip dest-ip-addr** *dest-ip-addr* {**interface** *interface* | **interface** *interface* [**service instance** *efp-id* | **vrf** *vrf_id*} **Example:** `Device(config-ip-sla))# service-performance type ip dest-ip-addr 194.168.1.1 interface gigabitEthernet0/0/10 service instance 10`	Specifies the service performance type as IP and the destination IP address. Specifies the target for the SLA session. The options are: • service instance • interface • vrf

	Command or Action	Purpose
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iteration.
Step 6	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.
Step 7	**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 8	**default** | **exit** | **no** | **outer-vlan** | **packet-size** | **source-ip-addr** **Example:** `Device(config-ip-sla-service-performance-packet)#src-ip-addr 193.168.1.1`	Specifies the packet type. The options are: • **default** - Sets a command to its defaults. • **exit** - Exists the packet mode. • **no** - Negates a command or sets its defaults. • **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **src-ip-addr** - Specifies the source IP address. **Note** Ensure that the value of the configured packet profile matches the target configuration of the session.
Step 9	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the IP SLA Service Performance packet mode.
Step 10	**profile traffic direction** [**internal**] **cir** *number* or **eir** *number* or **cbs** *number* or **ebs** *number* or **conform-color set-dscp-transmit** *dscp_value* or **exceed-color**	Specifies the in-line traffic profile or selection of a pre-configured traffic profile. A traffic profile defines an upper bound on the volume of the expected service frames belonging to a particular service instance. If a traffic profile

	Command or Action	Purpose

	set-dscp-transmit *dscp_value* or **default** or **exit** or **no** or **rate step kbps | pps** *number*
	
	Example:
	
	`Device(config-ip-sla-service-performance)# profile traffic direction internal`
	`Device(config-ip-sla-service-performance-traffic)# cir 45000`
	`Device(config-ip-sla-service-performance-traffic)# eir 45000`
	`Device(config-ip-sla-service-performance-traffic)# conform-color set-dscp-transmit af43`
	`Device(config-ip-sla-service-performance-traffic)# exceed-color set-dscp-transmit af41`
	`Device(config-ip-sla-service-performance-traffic)# rate-step kbps 1000`
		is not specified, the Service Performance probe is in passive measurement mode.
		
		• **cir** - It is the Committed Information Rate.
		• **cbs** - It is the Committed Burst Size.
		• **conform-color** - Sets the color conform.
		• **default** - Sets a command to its defaults.
		• **drop** - Drops the packet.
		• **eir** - It is Excess Information Rate.
		• **ebs** - It is the Excess Burst Size.
		• **exceed-color** - Sets the color-exceed.
		• **exit** - Exits the traffic mode.
		• **no** - Negates a command or sets its defaults.
		• **rate step kbps** - Sets the rate step.
		• **set-dscp-transmit** *dscp_value* - Sets the IP DSCP value to a new value and sends the packet. The valid range is from 0 to 63. You also can enter nemonic name for a commonly used value.
		• **transmit** - Sends the packet without altering it. This is the default value.
		
		Note This command is required to configure the **rate step kbps** command.
		
		• **default** - Sets a command to its defaults.
		• **rate step kbps** - Specifies the transmission rate in kbps. The rate-step range is from 1 to 1000000 (1 Kbps to 1 Gbps).
		• **rate step pps** - Specifies the transmission rate in pps. The rate-step range is from 1 to 1000000 (1 pps to 1000000 pps).
		
		Note The **rate-step kbps | pps number** is mandatory for traffic generation to happen.

Example

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 vrf 2
frequency iteration 1 delay 1
duration time 50
profile packet
source-ip-addr 193.168.1.1
packet-size 512
profile traffic direction internal
cir 45000
eir 45000
cbs 45000
ebs 45000
rate-step kbps 50000 90000
conform-color set-dscp-transmit af43
exceed-color set-dscp-transmit af41
```

Configuring IP Target Color Blind Traffic Generation

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

Procedure

	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 ip dest-ip-addr** *dest-ip-addr* {**interface** *interface* | **bridge domain** *domain_id* | **interface** *interface* [**service instance** *efp-id* | **vrf** *vrf_id*} **Example:** `Device(config-ip-sla)# service-performance type ip dest-ip-addr 194.168.1.1 interface gigabitEthernet0/0/10 service instance 10`	Specifies the service performance type as IP and the destination IP address. Specifies the target for the SLA session. The options are: • service instance • interface • vrf • bridge domain

	Command or Action	Purpose
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iteration.
Step 6	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Sets the service performance duration configuration.
Step 7	**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 8	**default** | **exit** | **no** | **outer-vlan** | **packet-size** | **source-ip-addr** **Example:** `Device(config-ip-sla-service-performance-packet)#src-ip-addr 193.168.1.1`	Specifies the packet type. The options are: • **default** - Sets a command to its defaults. • **exit** - Exists the packet mode. • **no** - Negates a command or sets its defaults. • **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **src-ip-addr** - Specifies the source IP address. **Note** Ensure that the value of the configured packet profile matches the target configuration of the session.
Step 9	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the IP SLA Service Performance packet mode.
Step 10	**profile traffic direction internal** **Example:** `Device(config-ip-sla-service-performance)# profile traffic direction internal`	Specifies the in-line traffic profile or selection of a pre-configured traffic profile. A traffic profile defines an upper bound on the volume of the expected service frames belonging to a particular service instance. If a traffic profile

	Command or Action	Purpose
		is not specified, the Service Performance probe is in passive measurement mode.
Step 11	**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 to 1000000 (1 Kbps to 1 Gbps). • **rate step pps** - Specifies the transmission rate in pps. The rate-step range is from 1 to 1000000 (1 pps to 1000000 pps). **Note** The command **rate-step kbps | pps number** is mandatory for traffic generation.

Example

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 vrf 2
frequency iteration 1 delay 1
duration time 50
profile packet
source-ip-addr 193.168.1.1
packet-size 512
profile traffic direction internal
rate-step kbps 50000 90000
```

Configuring IP Target Color Blind Passive Measurement

Perform the following steps to configure IP target color blind passive measurement.

Procedure

	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** *sla_id* **Example:** `Device(config)# ip sla 100`	Specifies the SLA ID to start the IP SLA session.
Step 4	**service-performance type ip dest-ip-addr** *dest_ip_addr* {**interface** *interface* | **bridge domain** *domain_id* | **interface** *interface* [**service instance** *efp-id*] | **vrf** *vrf_id*} **Example:** `Device(config-ip-sla)# service-performance type ip dest-ip-addr 194.168.1.1 interface gigabitEthernet0/0/10 service instance 10`	Specifies the service performance type as IP and the destination IP address. Specifies the target for the SLA session. The options are: • service instance • interface • vrf • bridge domain
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iteration.
Step 6	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Sets the service performance duration configuration.
Step 7	**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 8	**default** | **exit** | **no** | **packet-size** | **source-ip-addr** **Example:** `Device(config-ip-sla-service-performance-measurement)# throughput`	Specifies the measurement type based on which the service performance is calculated. The options are: • **default** - Sets a command to its default values. • **exit** - Exists the packet mode. • **no** - Negates a command or sets its defaults. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, and 9216 bytes. • **source-ip-addr** - Specifies the source IP address.

	Command or Action	Purpose
Step 9	**measurement-type direction internal** **Example:** `config-ip-sla-service-performance)#measurement-type direction internal`	Specifies the direction of measurement.
Step 10	**default** | **exit** | **loss** | **throughput** | **receive** **Example:** `Device(config-ip-sla-service-performance-measurement)# throughput`	Specifies the measurement type based on which the service performance is calculated. The options are: • **default** - Sets a command to its default values. • **loss** - Specifies the measurement such as frame loss. • **throughput** - Specifies the measurement such as average rate of successful frame delivery. • **receive** - Specifies the passive measurement mode.

Example

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 vrf 2
frequency iteration 1 delay 1
duration time 50
measurement-type direction internal
receive
profile packet
source-ip-addr 193.168.1.1
packet-size 512
```

Configuring IP Target Two-Way Color-Aware Session

Perform the following steps to configure IP target two-way color-aware session.

Note The default **frequency iteration** command value may cause the **duration** command to be rejected for higher values. In this case, the **frequency iteration** command is recommended before the execution of the **duration** command.

Procedure

	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 ip dest-ip-addr** *dest-ip-addr* {**interface** *interface* | **interface** *interface* [**service instance** *efp-id* | **vrf** *vrf_id*} **Example:** `Device(config-ip-sla)# service-performance type ip dest-ip 194.168.1.1 interface gigabitEthernet0/0/10 service instance 10`	Specifies the service performance type as IP and the destination IP address. Specifies the target for the SLA session. The options are: • service instance • interface • vrf
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iteration.
Step 6	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Sets the service performance duration configuration.
Step 7	**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 8	**deafult** | **exit** | **no** | **outer vlan** | **packet-size** | **source-ip-addr** **Example:** `Device(config-ip-sla-service-performance-packet)# src-ip-addr 193.168.1.1`	Specifies the packet type. The options are: • **default** - Sets a command to its defaults. • **exit** - Exists the packet mode. • **no** - Negates a command or set its defaults.

	Command or Action	Purpose
		• **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64, 128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. • **source-ip-addr** - Specifies the source IP address. **Note** Ensure that the value of the configured packet profile matches the target configuration of the session.
Step 9	**exit** **Example:** `Device(config-ip-sla)# exit`	Exists the IP SLA Service Performance packet mode.

Step 10	**profile traffic direction internal cir** *number* or **eir** *number* or **cbs** *number* or **ebs** *number* or **conform-color set-dscp-transmit** *dscp_value* or **exceed-color set-dscp-transmit** *dscp_value* or **default** or **exit** or **no** or **rate step kbps | pps** *number*
	Example:
	`Device(config-ip-sla-service-performance)# profile traffic direction internal`
	`Device(config-ip-sla-service-performance-traffic)# cir 45000`
	`Device(config-ip-sla-service-performance-traffic)# eir 45000`
	`Device(config-ip-sla-service-performance-traffic)# conform-color set-dscp-transmit af434`
	`Device(config-ip-sla-service-performance-traffic)# exceed-color set-dscp-transmit af41`
	`Device(config-ip-sla-service-performance-traffic)# rate-step kbps 1000`
		Specifies the in-line traffic profile or selection of a pre-configured traffic profile. A traffic profile defines an upper bound on the volume of the expected service frames belonging to a particular service instance. If a traffic profile is not specified, the Service Performance probe is in passive measurement mode.
		• **cir** - It is the Committed Information Rate.
		• **cbs** - It is the Committed Burst Size.
		• **conform-color** - Sets the color conform.
		• **default** - Sets a command to its defaults.
		• **drop** - Drops the packet.
		• **eir** - It is Excess Information Rate.
		• **ebs** - It is the Excess Burst Size.
		• **exceed-color** - Sets the color-exceed.
		• **exit** - Exits the traffic mode.
		• **no** - Negates a command or sets its defaults.
		• **rate step kbps** - Sets the rate step.

	Command or Action	Purpose
		• **set-dscp-transmit** *dscp_value* - Sets the IP DSCP value to a new value and sends the packet. The valid range is from 0 to 63. You also can enter nemonic name for a commonly used value. • **transmit** - Sends the packet without altering it. This is the default value. **Note** This command is required to configure the **rate step kbps** command. • **default** - Sets a command to its defaults. • **rate step kbps** - Specifies the transmission rate in kbps. The rate-step range is from 1 to 1000000 (1 Kbps to 1 Gbps). • **rate step pps** - Specifies the transmission rate in pps. The rate-step range is from 1 to 1000000 (1 pps to 1000000 pps). **Note** The **rate-step kbps | pps number** is mandatory for traffic generation.
Step 11	**measurement-type direction internal conform-color dscp** *dscp_value* **exceed-color dscp** *dscp_value* **Example:** `Device(config-ip-sla-service-performance)# measurement-type direction internal conform-color dscp af43 exceed-color dscp af41`	Specifies the direction of measurement.
Step 12	**default** | **exit** | **loss** | **no** | **throughput** | **receive** | **delay** | **jitter**	Specifies the measurement type based on which the service performance is calculated. The options are: • **default** - Sets a command to its default value. • **loss** - Specifies the measurement such as frame loss. • **throughput** - Specifies the measurement such as average rate of successful frame delivery. • **receive** - Specifies the passive measurement mode.

	Command or Action	Purpose
		• **delay** - Specifies the measurement that is frame delay (FTD). • **jitter** - Specifies the measurement that is frame delay variation (FDV).

Example

```
ip sla 1
 service-performance type ip dest-ip-addr 150.1.1.2 interface TenGigabitEthernet0/0/3 service
 instance 1
  frequency iteration 1 delay 1
 measurement-type direction internal conform-color dscp af11 exceed-color dscp af12
   loss
   receive
   throughput
   delay
   jitter
   profile packet
   source-ip-addr 2.2.1.2
   packet-size 512
   outer-vlan 10
  profile traffic direction internal
   cir 100000
   eir 100000
   rate-step kbps 200000
   conform-color set-dscp-transmit af11
   exceed-color set-dscp-transmit af12
  duration time 1200
```

Configuring IP Target Color-Aware IMIX Traffic Generation

Perform the following steps to configure IP target color-aware IMIX traffic generation session.

Procedure

	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.

	Command or Action	Purpose
Step 4	**service-performance type ip dest-mac-addr** *dest_ip_addr* {**interface** *interface* | **interface** *interface* [**service instance** *efp-id*] | **vrf** *vrf_id*} **Example:** `Device(config-ip-sla))#service-performance type ip dest-ip-addr 194.168.1.1 interface gigabitEthernet0/0/10 service instance 10`	Specifies the service performance type as IPt and the destination IP address. Specifies the target for the SLA session. The options are: • service instance • interface • vrf
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iterations.
Step 6	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.
Step 7	**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 8	**default** | **exit** | **no** | **packet-size imix** | **source-ip-addr** **Example:** `Device(config-ip-sla-service-performance-packet)#packet-size imix`	Specifies the packet type. The options are: • **default** - Sets a command to its defaults. • **exit** - Exists the packet mode. • **no** - Negates a command or set its default. • **packet-size** - Specifies the packet size in bytes; the default size is 64. The supported packet sizes are 64,128, 256, 512, 1024, 1280, 1518, 9216 bytes, and IMIX. **Note** For IMIX, the packet-size should be explicitly mentioned as IMIX. • **source-ip-addr** - Specifies the source IP address. **Note** Ensure that the value of the configured packet profile matches the target configuration of the session.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the profile packet mode.

Step 10	**profile packet direction internal cir** *number* or **eir** *number* or **cbs** *number* or **ebs** *number* or **conform-color set-dscp-transmit** *dscp_value* or **exceed-color set-dscp-transmit** *dscp_value* or **default** or **exit** or **no** or **rate step kbps**
	Example:
	`Device(config-ip-sla-service-performance)#profile traffic direction internal`
	`Device(config-ip-sla-service-performance-traffic)# cir 45000`
	`Device(config-ip-sla-service-performance-traffic)# eir 45000`
	`Device(config-ip-sla-service-performance-traffic)# conform-color set-dscp-transmit af43`
	`Device(config-ip-sla-service-performance-traffic)# exceed-color set-dscp-transmit af41`
	`Device(config-ip-sla-service-performance-traffic)# rate-step kbps 1000`
		Specifies the in-line traffic profile or enables the selection of a pre-configured traffic profile. A traffic profile defines an upper limit on the volume of the expected service frames belonging to a particular service instance. If a traffic profile is not specified, the Service Performance probe is in passive measurement mode.
		• **cir** - It is the Committed Information Rate.
		• **cbs** - It is the Committed Burst Size.
		• **conform-color** - Sets the conform color.
		• **default** - Sets a command to its defaults.
		• **drop** - Drops the packet.
		• **eir** - It is the Excess Information rate.
		• **ebs** - It is the Excess Burst Size.
		• **exceed-color** - Sets the exceed color.
		• **exit** - Exits the traffic mode.
		• **no** - Negates a command or sets its defaults.
		• **rate step kbps** - Sets the rate step.
		• **set-cos-transmit** *cos_value* - Sets the CoS value to a new value, and sends the packet. The valid range is from 0 to 7.
		• **transmit** - Sends the packet without altering it. This is the default value.
		Note This command is required to configure the rate step kbps command.
		• **default** - Sets a command to its defaults.

Step 11	**default** or **exit** or **no** or **rate step kbps**	Specifies the traffic type. The options are: • **default**: Set a command to its default value.

	Command or Action	Purpose
		• **rate step kbps**: Specifies the transmission rate in kbps. The rate-step range is from 1-1000000 (1 Kbps to 1Gbps).

Example

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 vrf 2
frequency iteration 1 delay 1
duration time 50
profile packet
source-ip-addr 193.168.1.1
packet-size imix
profile traffic direction internal
cir 45000
eir 45000
cbs 45000
ebs 45000
rate-step kbps 50000 90000
conform-color set-dscp-transmit af43
exceed-color set-dscp-transmit af41
```

Configuration Examples for Configuring Y.1564 t o Generate and Measure IP Traffic

This section shows sample configurations for IP traffic generation and measurement.

Example: Passive Color-Aware Measurement Session

The following is a sample configuration for passive color-aware measurement session.

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 interface TenGigabitEthernet0/0/3
service instance 1
frequency iteration 1 delay 1
duration time 50
measurement-type direction internal
conform-color dscp af43
exceed-color dscp af41
receive
profile packet
source-ip-addr 193.168.1.1
packet-size 512
```

Example: Color-Aware IMIX — Traffic Generation

The following is a sample configuration for color-aware IMIX — traffic generation session.

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 interface TenGigabitEthernet0/0/3
```

```
service instance 1
frequency iteration 1 delay 1
duration time 50
profile packet
source-ip-addr 193.168.1.1
packet-size imix
profile traffic direction internal
cir 45000
eir 45000
cbs 45000
ebs 45000
rate-step kbps 50000 90000
conform-color set-dscp-transmit af43
exceed-color set-dscp-transmit af41
```

Example: Color-Aware — Traffic Generation

The following is a sample configuration for color-aware — traffic generation session.

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 interface TenGigabitEthernet0/0/3
frequency iteration 1 delay 1
duration time 50
profile packet
source-ip-addr 193.168.1.1
packet-size 512
profile traffic direction internal
cir 45000
eir 45000
cbs 45000
ebs 45000
rate-step kbps 50000 90000
conform-color set-dscp-transmit af43
exceed-color set-dscp-transmit af41
```

Example: Color Blind — Traffic Generation

The following is a sample configuration for a color blind — traffic generation session.

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 bridge-domain 100
frequency iteration 1 delay 1
duration time 50
profile packet
source-ip-addr 193.168.1.1
packet-size 512
profile traffic direction internal
rate-step kbps 50000 90000
```

Example: Color Blind — Passive Measurement

The following is a sample configuration for a color blind — passive measurement session.

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 vrf 2
frequency iteration 1 delay 1
duration time 50
measurement-type direction internal
```

```
receive
profile packet
source-ip-addr 193.168.1.1
packet-size 512
```

Example: Color-Aware — Two Way

The following is a sample configuration for a color-aware — two way session.

```
ip sla 1
 service-performance type ip dest-ip-addr 150.1.1.2 interface TenGigabitEthernet0/0/3 service
 instance 1
  frequency iteration 1 delay 1
 measurement-type direction internal conform-color dscp af11 exceed-color dscp af12
   loss
   receive
   throughput
   delay
   jitter
   profile packet
   source-ip-addr 2.2.1.2
   packet-size 512
   outer-vlan 10
  profile traffic direction internal
   cir 100000
   eir 100000
   rate-step kbps 200000
   conform-color set-dscp-transmit af11
   exceed-color set-dscp-transmit af12
  duration time 100
```

Example: Color Blind — Two Way

The following is a sample configuration for a color blind — two way session.

```
ip sla 1
 service-performance type ip dest-ip-addr 150.1.1.2 interface TenGigabitEthernet0/0/3 service
 instance 1
  frequency iteration 1 delay 1
 measurement-type direction internal
   loss
   receive
   throughput
   delay
   jitter
   profile packet
   source-ip-addr 2.2.1.2
   packet-size 512
   outer-vlan 10
  profile traffic direction internal
   rate-step kbps 200000
  duration time 100
```

Example: Configuring Y1564 Traffic Payload Pattern

The following is a sample configuration for a Y1564 Traffic Payload Pattern:

```
ip sla 101
service-performance type ethernet dest-mac-addr 0012.1212.1221 interface
TenGigabitEthernet0/3/1 service instance 100
signature 32
measurement-type direction external
throughput
profile packet
src-mac-addr 4055.3989.7b56
profile traffic direction external
rate-step kbps 1000
duration time 60
```

How to Configure IP (Layer 3) Loopback on Responder

This section shows how to configure IP (Layer 3) loopback on responder.

Enabling IP SLA Loopback on Responder

Perform the following steps to configure ethernet target traffic generation.

Note For layer 3 Loopback, the parameters **dest-ip-addr** and **src-ip-addr** are mandatory, otherwise the configuration fails. **Outer-vlan** is mandatory only for Trunk EFP and optional for other interface types.

Procedure

	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 ip dest-ip-addr** *dest-ip-addr* **interface** *interface* **Example:** `Device(config-ip-sla))#service-performance type ip dest-ip-addr 194.168.1.1 interface gigabitEthernet0/0/1`	Specifies the service performance type as IP and the destination IP address. Specifies the target for the SLA session. The options are: • service instance • interface

	Command or Action	Purpose
		• vrf • bridge-domain
Step 5	**frequency iteration** *number* **delay** *number* **Example:** `Device(config-ip-sla)# frequency iteration 1 delay 2`	Specifies the number of interactions and delay between the iteration.
Step 6	**loopback direction** {*internal*} **Example:** `Device(config-ip-sla)# loopback direction internal`	Configures loopback direction.
Step 7	**duration time** *seconds* **Example:** `Device(config-ip-sla)# duration time 30`	Specifies the time period to send packets.
Step 8	**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 9	**source-ip-addr** *ip-address* | **outer-vlan** *vlan-id*
	Example:
	`Device(config-ip-sla-service-performance-packet)# source-ip-addr 51.1.1.1`
	`Device(config-ip-sla-service-performance-packet)# outer-vlan 301`
		Specifies the packet type. The options are:
		• **default** - Sets a command to its defaults.
		• **exit** - Exists the packet mode.
		• **no** - Negates a command or set its defaults.
		• **source-ip-addr** - Specifies the source IP address.
		• **outer-vlan** - Specifies the VLAN ID that is populated in the outer VLAN tag of the packet.
		Note Ensure that the value of the configured packet profile matches the target configuration of the session.

Step 10	**exit** **Example:** `Device(config-ip-sla-service-performance-packet)#exit`	Exits the profile packet mode.

Example

```
ip sla 1
service-performance type ip dest-ip-addr 194.168.1.1 interface gi0/0/0 service instance 1
frequency iteration 1 delay 1
loopback direction internal
profile packet
source-ip-addr 193.168.1.1
outer-vlan 301
duration time 30000
```

SADT Overhead Accounting

FPGA measures the following parameters for SADT:

- Throughput
- Frame Loss
- Jitter
- Delay

FPGA has the capability to generate and measure only 1Gbps traffic rate and hence maximum throughput cannot be achieved.

The following table shows the packet size and the maximum rate that can be achieved.

Packet Size (Bytes)	1G Maximum Rate (kbps)
64	469848
128	638061
256	775123
512	867758
1024	922728
1280	934554
1518	942124
9216	977675
IMIX	788000

To overcome this limitation, use the **platform y1564 shadow-session-enable** command to replicate the packets 10 times in FPGA.

Restrictions

- If two SADT sessions are run in parallel with the same source and destination MAC address by fault, then subsequent SADT session must be started only after modifying the source and destination MAC addresses in the SLA profile to overcome loss.
- The platform y1564 **shadow-session-enable** command does not work in HA setup.
- While using platform y1564 **shadow-session-enable** command, SADT session uses a shadow session with the given MAC + 1 (for example, 0011.1111.2222 to 0011.1111.2223). Hence source MAC and destination MAC must not be in consecutive numbers.
- Use external Ethernet data plane loopback (ELB) for this feature as 1G internal loopback is not supported.
- 1G internal SADT only supports EFP cross connect EFP.
- 1G SADT is *not* supported on local connect and layer 2 VFI.
- Color-aware configurations are *not* supported on 1G SADT.
- 1G SADT can *only* be configured in two-way mode.
- 1G SADT target type is *only* supported on access EFP.
- A combination of 1G and 10G SADT sessions cannot be performed in parallel. Also, two 10G SADT sessions cannot be performed in parallel.
- SADT statistics can *only* be validated after SADT operation is complete.
- Layer 3 packets are *not* supported when SADT overhead accounting is enabled.
- You should configure the parameters that are *only* related to layer 2 for a packet profile.
- Overall throughput value slightly differs the rate step value.
- Multiple rate steps of a single command should be added in an incremental order.
- While QoS egress shaper policy is applied on the same SAT interface with 1G SADT, SAT traffic generation is affected based on the shaper value. There is no effect on the traffic when inbound policer-based policy is applied on the same SAT interface.
- Broadcast and multicast destination MAC are *not* supported.
- You should define the rate-steps upper limits of SADT to provide bandwidth to BFD and avoid the OSPF flaps.
- Online Insertion and Removal (OIR) and Stateful Switchover (SSO) are *not* supported. SLA session must be stopped and re-started manually after these triggers are generated.
- SADT SLA session and ELB on the same service instance of an interface are *not* supported.
- 1G SADT on encapsulation default does not work when untagged encapsulation is configured on the interface.
- 1G SADT is *not* supported on VRF and Port-Channel interfaces.

Configuring SADT Overhead Accounting

To configure SADT Overhead Accounting:

```
enable
configure terminal
platform y1564 shadow-session-enable
```

To remove the configuration:

```
enable
configure terminal
no platform y1564 shadow-session-enable
```

Verifying SADT Overhead Accounting Configuration

Use **show ip sla st 101** command to verify SADT overhead accounting configuration as follows:

```
Router#show ip sla st 101
IPSLAs Latest Operation Statistics

IPSLA operation id: 101
Type of operation: Ethernet Service Performance
Test mode: Two-way Measurement
Steps Tested (kbps): 500000
Test duration: 30 seconds

Latest measurement:  *14:42:45.333 UTC Thu Jan 9 2020
Latest return code:  OK

Overall Throughput: 500000 kbps

Step 1 (500000 kbps):
Stats:
IR(kbps)  FL          FLR      Avail    FTD Min/Avg/Max      FDV Min/Avg/Max
500000    0           0.00%    100.00%  32.96us/196.06us/198.96us  160ns/855ns/163.28us
Tx Packets: 28409091  Tx Bytes: 1875000006
Rx Packets: 28409091  Rx Bytes: 1875000006
Step Duration: 30 seconds
```

Configurable User-Defined and EMIX Packet Size

Table 18: Feature History

Feature Name	Release	Description
Configurable Y.1564 Service Activation Frame Sizes and EMIX Support	Cisco IOS XE Amsterdam 17.3.1	Starting with Cisco IOS XE Amsterdam 17.3.1 release, EMIX packet size is supported. For EMIX traffic, packet sizes of 64, 128, 256, 1024 and 1518 bytes are supported. These packet sizes are forwarded in ratio of 1:1:1:1:1.

Feature Name	Release	Description
SAT based support for configurable EMIX traffic pattern in FPGA	Cisco IOS XE Bengaluru 17.4.1	The support for EMIX packet size is enhanced. For EMIX traffic, packet sizes of 64, 128, 256, 512, 1024, 1280, 1518, Maximum Transmission Unit (MTU) and user-defined patterns are supported. These packet sizes are forwarded in ratio of 1:1:1:1:1.
EMIX Sequence Enhancement	Cisco IOS XE Bengaluru 17.4.1	This feature enables SAT based support for configurable EMIX traffic pattern in FPGA-based SAT.
Configurable User-Defined and EMIX Packet Size	Cisco IOS XE Bengaluru 17.4.1	This feature allows you to configure user-defined and Enterprise traffic (EMIX) packet sizes. Use the following commands to configure user-defined and EMIX packet sizes: • **packet-size user-defined** *packet size* • **packet-size emix sequence** *emix-sequence* [**u-value** *u-value value*]

EMIX patterns are to be specified by the size designator for each frame in the repeating pattern. The following table is an example of the EMIX test profile.

Starting with Cisco IOS XE Release 16.12.4, EMIX packet size (default abceg pattern) is supported. For EMIX traffic, ITU-T Rec. Y.1564 packet sizes of 64, 128, 256, 1024, and 1518 bytes are supported.

The following table shows the configurable packet size patterns. You must specify the EMIX patterns using the size designator for each frame in the repeating pattern. For example, in the above table, you can specify an eight-frame repeating pattern as follows:

Table 19: Configuring EMIX Frame Size

EMIX Definition	a	b	c	d	e	f	g	h	(u) User Defined
EMIX size (in bytes)	64	128	256	512	1024	1280	1518	Service MTU	Range is from 64-9216

Note SAT traffic is not transmitted as per the configured emix sequence order on the router.

- Starting with Cisco IOS XE Amsterdam 17.3.1 release, EMIX packet size (default abceg pattern) is supported . For EMIX traffic, ITU-T Rec. Y.1564 packet sizes of 64, 128, 256, 1024, and 1518 bytes are supported.
- The IP SLA packets are generated and forwarded in ratio of 1:1:1:1:1 from UNI or NNI port based on your configuration.
- Starting from Cisco IOS XE Bengaluru 17.4.1 release, EMIX packet size of 62, 128, 256, 512, 1024, 1280, 1518, MTU and *user-defined* bytes are supported. You can configure the SLA using Maximum Transmission Unit (MTU) of Ethernet interface.

  A maximum of eight characters in the **packet-size emix sequence abcdefgh** command is supported. In case you want to use **u**, then you must include **u-value** in the command.
- You can specify the packet size according to Y1564 and assign the user-specified MTU using a hex pattern (**abcdefghu**).
  - EMIX – **abcdefghu** = 64, 128, 256, 512, 1024, 1280, 1518, MTU, *user-defined*

    EMIX – **aabbccuu** = 64, 64, 128, 128, 256, 256, *user-defined*, *user-defined*
- The EMIX pattern must be configurable for the service test.
- Data loss equal to the egress MTU drop is observed when Y1564 is used to configure BDI and h in EMIX sequence.
- EMIX sequence is supported with platform **platform y1564 shadow-session enable** command.
- When the **platform y1564 shadow-session enable** command is enabled, you cannot configure two parallel sessions for 1G interface.

Configuration Example: Configurable User-Defined and EMIX Packet Size

The following example shows the configuration of user-defined packet size:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip sla 1
Router(config-ip-sla)#service-performance type ethernet dest-mac-addr aaa.ccc.aaa interface
 Gi0/1
Router(config-ip-sla-service-performance)#profile packet
Router(config-sla-service-performance-packet)#packet-size ?
  1024          1024 byte
  128           128 byte
  1280          1280 byte
  1518          1518 byte
  256           256 byte
  512           512 byte
  64            64 byte
  9216          9216 byte
  emix          Emix packet size
  imix          Imix packet size
  user-defined  User defined Packet Size
Router(config-sla-service-performance-packet)#packet-size user-defined 2955
Router(config-sla-service-performance-packet)#end
```

The following example shows the configuration of EMIX packet size:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)#ip sla 1
Router(config-ip-sla)#service-performance type ethernet dest-mac-addr aaa.ccc.aaa interface
 Gi0/1
Router(config-ip-sla-service-performance)#profile packet
Router(config-sla-service-performance-packet)#packet-size ?
  1024  1024 byte
  128   128 byte
  1280  1280 byte
  1518  1518 byte
  256   256 byte
  512   512 byte
  64    64 byte
  9216  9216 byte
  emix  Emix packet size
  imix  Imix packet size

Router(config-sla-service-performance-packet)#packet-size em
Router(config-sla-service-performance-packet)#packet-size emix ?
  sequence  Specify the EMIX sequence
  <cr>      <cr>

Router(config-sla-service-performance-packet)#packet-size emix sequence ?
  WORD  EMIX Sequence

Router(config-sla-service-performance-packet)#packet-size emix sequence aaabbcc ?
 u-value  Specify the user-defined value
  <cr>     <cr>

Router(config-sla-service-performance-packet)#packet-size emix sequence aaabbbccu u-value
?
  <64-10236>  Specify user-defined packet size value

Router(config-sla-service-performance-packet)#packet-size emix sequence aaabbbccu u-value
128 ?
  <cr>  <cr>
```

Verification of User-Defined and EMIX Packet Size Configuration

Use **show run | sec sla** command to verify user-defined packet size configuration.

```
Router# show run | sec sla
ip sla 100
service-performance type ethernet dest-mac-addr aaaa.bbbb.cccc interface GigabitEthernet0/1

  profile packet
   packet-size user-defined 2955
```

Use **show run | sec sla** command to verify EMIX packet size configuration.

```
Router#show run | section sla
ip sla 1
service-performance type ethernet dest-mac-addr 0aaa.0ccc.0aaa interface GigabitEthernet0/1

  profile packet
   packet-size emix sequence aabbccu u-value 128
```

SADT over VC When Access Interface is Down

Table 20: Feature History

Feature Name	Release Information	Description
SADT over VC when Access Interface is Down	Cisco IOS XE Dublin 17.10.1	You can perform Service Activation and Deactivation (SADT) over Virtual Circuit (VC) even when access interface is down.

When a PE router isn't connected to a CE router, and an access interface is down, and hence the VC is down. You can't perform SAT over VC during such situation.

SADT over VC when access interface is down, is supported only on the ASR 920 and RSP2 platforms.

The following scenario enables you to perform SAT over VC even when the access interface is down.

- Node A and Node B are two pseudowire endpoints. IP SLA is configured on the pseudowire access interface OF Node A. Ethernet Data Plane Loopback (EDPL) is configured on the pseudowire access interface on Node B.
- IP SLA traffic is initiated from the pseudowire access interface on Node A. This traffic is be transported over pseudowire and reaches Node B. On Node B, EDPL associated with the pseudowire access interface is looping back the traffic on pseudowire.
- IP SLA receive statistics on Node A helps validating various parameters of SAT.
- You can perform SAT over this VC even though there's no CE connected to these access interfaces.
- You can bring up the VC using the **platform** command. Once the VC comes up, EDPL and IP SLA associated with the pseudowire access interfaces can be started. We recommend that you disable the **platform** command once testing is complete.

Limitations for SADT Over VC Feature

- SADT over HSPW is not supported

Configuring SADT and Pseudowire Circuit

The configuration steps involve the following procedure:

- Configure and bring up an ISIS or OSPF Network
- Configure pseudowire
- Enable the **platform** command and verify the VC status.
- Configure SADT
- Verify the SADT and pseudowire status

On router 1, perform the following configuration:

Ensure that you enable the **platform** command and verify the VC status before configuring IPSLA.

```
IP SLA:
Router 1
ip sla 2
 service-performance type ethernet dest-mac-addr 0000.0005.0055 interface
TenGigabitEthernet0/0/1 service instance 3503
  frequency time 604800
  description SADT2
  measurement-type direction internal

   loss
   receive
   throughput
  profile packet
   outer-cos 2
   outer-vlan 3503
   packet-size 1518
   src-mac-addr 0000.0004.0044
  profile traffic direction internal
   rate-step kbps 1000
  duration time 1000
```

```
IP SLA:
Router 1
interface TenGigabitEthernet0/0/1
 service instance 3503ethernet
  encapsulation dot1q 3503
  rewrite ingress tag pop 1 symmetric
  xconnect 11.11.11.11 13 encapsulation mpls
```

Enable SADT

```
ip sla schedule 2 life forever start-time now
```

```
Router2#
interface GigabitEthernet0/0/18
service instance 3503 ethernet
  encapsulation dot1q 3503
  xconnect 22.22.22.22 13 encapsulation mpls
  ethernet loopback permit internal
```

Activate ELB

```
ethernet loopback start local interface gigabitEthernet 0/0/18 service instance 3503 internal
 dot1q 3503 timeout none
```

Verifying SADT and Pseudowire Circuit

```
Router1#show ip interface te 0/0/1
TenGigabitEthernet0/0/1 is down, line protocol is down
  Internet protocol processing disabled
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router1(config)#platform y1564 enable-interface te 0/0/1
Router1(config)#
Aug 25 08:44:57.132: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/1, changed state to
up
Aug 25 08:44:57.135: %IOSXE_RP_ALARM-6-INFO: cleared CRITICAL TenGigabitEthernet0/0/1:
Physical Port Link Down
Aug 25 08:44:57.163: %NETCLK-6-SRC_UPD: Synchronization source TenGigabitEthernet0/0/1
status (Signal Failure clear) is posted to all selection process.
Aug 25 08:44:57.831: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/1,
 changed state to up
Router1(config)#end

Router1#show ip interface te 0/0/1
TenGigabitEthernet0/0/1 is up, line protocol is up
  Internet protocol processing disabled


Router1#show ip sla statistics 2
IPSLAs Latest Operation Statistics

IPSLA operation id: 2
Type of operation: Ethernet Service Performance
Test mode: Two-way Measurement
Steps Tested (kbps): 1000
Test duration: 1000 seconds

Latest measurement:  15:30:07.387 IST Wed Aug 24 2022
Latest return code:  OK

Overall Throughput: 1008 kbps

Step 1 (1000 kbps):
Stats:
IR(kbps)  FL           FLR      Avail
1008      0            0.00%    100.00%
Tx Packets: 82895  Tx Bytes: 126000400
Rx Packets: 82895  Rx Bytes: 126000400
Step Duration: 1000 seconds
```

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

CHAPTER 11

IP SLA VCCV Operation

The IP SLA supports Virtual Circuit Connectivity Verification (VCCV) for pseudowire Emulation Edge-to-Edge (PWE3) services across MPLS networks. The IP SLAs VCCV operation type is based on the **ping mpls pseudowire** command, which checks MPLS LSP connectivity across an Any Transport over MPLS (AToM) virtual circuit (VC) by sending a series of pseudowire ping operations to the specified destination PE router.

MPLS LSP connectivity checking is performed using an IP SLAs VCCV operation (rather than through the **ping mpls** command with the **pseudowire** keyword). The VCCV operation provides IP SLA proactive threshold monitoring and multioperation scheduling capabilities.

Note IP SLA VCCV operation does not support LSP discovery.

- Configuring and Scheduling an IP SLA VCCV Operation, on page 151
- Example for Configuring an IP SLA VCCV Operation, on page 154

Configuring and Scheduling an IP SLA VCCV Operation

Procedure

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 777
```

Begins configuring an IP SLA VCCV operation and enters IP SLA configuration mode.

Step 4 **mpls lsp ping pseudowire** *peer-ipaddr vc-id* [**source-ipaddr** *source-ipaddr*]

Example:

```
Router(config-ip-sla)# mpls lsp ping
pseudowire 192.168.1.103 123 source-ipaddr 192.168.1.102
```

Configures the IP SLA VCCV operation as an LSP pseudowire ping and enters VCCV configuration mode.

Step 5 **exp** *exp-bits*

Example:

```
Router(config-sla-vccv)# exp 5
```

(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLA VCCV operation.

Step 6 **frequency** *seconds*

Example:

```
Router(config-sla-vccv)# frequency 120
```

(Optional) Specifies the rate at which a specified IP SLA VCCV operation repeats.

Step 7 **request-data-size** *bytes*

Example:

```
Router(config-sla-vccv)# request-data-size 200
```

(Optional) Specifies the protocol data size for a request packet of an IP SLA VCCV operation.

Step 8 **secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency*

Example:

```
Router(config-sla-vccv)# secondary-frequency connection-loss 10
```

(Optional) Sets the measurement frequency (secondary frequency) to which an IP SLA VCCV operation should change when a reaction condition occurs.

Step 9 **tag** *text*

Example:

```
Router(config-sla-vccv)# tag testgroup
```

(Optional) Creates a user-specified identifier for an IP SLA VCCV operation.

Step 10 **threshold** *milliseconds*

Example:

```
Router(config-sla-vccv)# threshold 6000
```

(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLA VCCV operation.

Step 11 **timeout** *milliseconds*

Example:

```
Router(config-sla-vccv)# timeout 7000
```

(Optional) Specifies the amount of time the IP SLA VCCV operation waits for a response from its request packet.

Step 12 **exit**

Example:

```
Router(config-sla-vccv)# exit
```

Exits VCCV configuration mode and returns to global configuration mode.

Step 13 **ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]

Example:

```
Router(config)# ip sla reaction-configuration 777 react connectionLoss threshold-type
consecutive 3 action-type traponly
```

(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLA VCCV Operation.

Step 14 **ip sla logging traps**

Example:

```
Router(config)# ip sla logging traps
```

(Optional) Enables the generation of SNMP system logging messages specific to IP SLA trap notifications.

Step 15 **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**]

Example:

```
Router(config)# ip sla schedule 777 life forever start-time now
```

Configures the scheduling parameters for an IP SLA VCCV operation.

Step 16 **exit**

Example:

```
Router(config)# exit
```

Exits global configuration submode and returns to privileged EXEC mode.

Example for Configuring an IP SLA VCCV Operation

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

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

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

```
ip sla 777
 mpls lsp ping pseudowire 192.168.1.103 123
  exp 5
  frequency 120
  secondary-frequency timeout 30
  tag testgroup
  threshold 6000
  timeout 7000
  exit
!
 ip sla reaction-configuration 777 react rtt threshold-value 6000 3000 threshold-type
immediate 3 action-type traponly
 ip sla reaction-configuration 777 react connectionLoss threshold-type immediate action-type
 traponly
 ip sla reaction-configuration 777 react timeout threshold-type consecutive 3 action-type
traponly
 ip sla logging traps
!
 ip sla schedule 777 life forever start-time now
 exit
```

RTT Thresholds

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

Connection Loss

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

Response Timeout

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