Extreme SLX-OS
Monitoring Configuration Guide, 20.7.3

Supporting ExtremeRouting and ExtremeSwitching
SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150,
Extreme 8820, Extreme 8720, and Extreme 8520

9039527-00 Rev AB
October 2026



Copyright © 2025 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

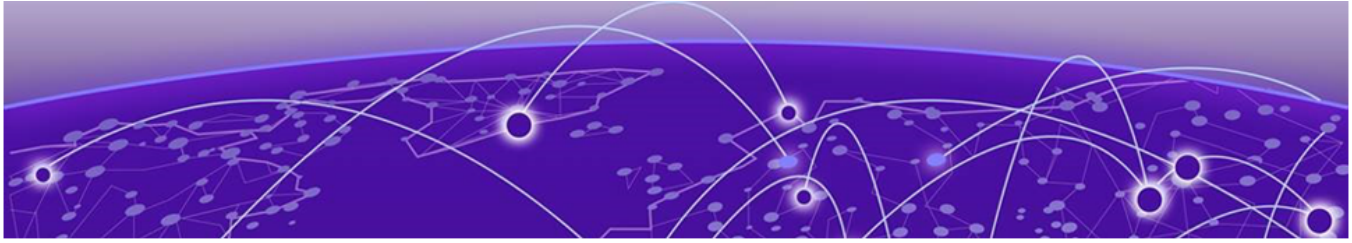


Table of Contents

Preface **6**
- Text Conventions 6
- Documentation and Training 7
  - Open Source Declarations 8
  - Training 8
- Help and Support 8
  - Subscribe to Product Announcements 9
- Send Feedback 9

About This Document **10**
- What's New in this Document 10
- Supported Hardware 11
- Regarding Ethernet interfaces and chassis devices 11

Operation, Administration, and Maintenance (OAM) **12**
- IEEE 802.1ag Connectivity Fault Management 12
  - Y.1731 feature set support over VLL 12
  - Ethernet OAM capabilities 13
  - IEEE 802.1ag purpose 14
  - IEEE 802.1ag hierarchical network management 14
  - Mechanisms of Ethernet IEEE 802.1ag OAM 15
  - 802.1ag Connectivity Fault Management 17
  - CFM over double tagged end-points 23
  - Monitoring the status of devices in a VPLS network in a Provider's Maintenance Domain 24
- Y.1731 Performance Monitoring 28
  - About Y.1731 Performance Monitoring 28
  - Two-way ETH-SLM and Two-way ETH-DM 29
  - Configuration considerations 35
  - Scalability considerations 36
  - Configuring Y.1731 Performance Monitoring 36
- IEEE 802.3ah Ethernet in First Mile 42
  - 802.3ah protocol in Ethernet 43
  - Feature support and limitations 43
  - How discovery works 44
  - How remote loopback works 44
  - Configuring Link OAM 44

Mirroring **47**
- Switched Port Analyzer (SPAN) 47
- Remote SPAN (RSPAN) 47
- Encapsulated Remote SPAN (ERSPAN) 48
- General Considerations when configuring SPAN/RSPAN/ERSPAN 48
  - Considerations for SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720 48

Considerations for SLX 9540 and SLX 9640 devices 50
Considerations for SLX 9740/Extreme 8820 devices 50
Flow Based Mirroring 50
Legacy Flow Based Mirroring Configuration 50
New Flow Based Mirroring Configuration 50
Configure SPAN Mirroring 51
Configuring Flow based SPAN 52
Configuring RSPAN Mirroring 53
Configuring Flow based RSPAN 54
Configuring ERSPAN Mirroring 55

Network-Elements Telemetry 57
Network-elements telemetry overview 57
Telemetry profiles 57
interface 57
system-utilization 58
Queue profiles 58
Configuring telemetry profiles 60
Configuring queue telemetry profiles 60
External-collector streaming 61
Configuring telemetry collectors 62
gRPC-server streaming 63
Configuring the gRPC telemetry server 64
Configuring SSL on the gRPC telemetry server 66

Hardware Monitoring 68
Hardware monitoring overview 68
System Resource Monitoring (SRM) 68
CPU, memory, and buffer monitoring 69
Optical monitoring 71
Disk space monitoring and management 94
Port Monitoring 95
Cyclic redundancy check (CRC) 97
High and Low watermarks for port utilization 98

Remote Monitoring 100
RMON overview 100
Configuring and managing RMON 100
Configuring RMON events 100
Configuring Message Rate Limiting Constraints for Threshold Monitoring 101
Configuring RMON alarm settings 102
Monitoring CRC errors 102

System Monitoring 103
System Monitor overview 103
Monitored components 103
Configuring System Monitor 106
Setting system thresholds 106
Setting state alerts and actions 107
Configuring e-mail alerts 107
Viewing system optical monitoring defaults 108
Viewing the area-wise optical monitoring current status 108

Displaying the device health status 108

Logging and tracing 109

Overview 109
RASLog 109
AuditLog 110
Syslog 111
Importing a syslog CA certificate 112
Viewing the syslog CA certificate 112
Verifying syslog CA certificates 112
Deleting a syslog CA certificate 112
LOGS over RELP 113

sFlow 115

sFlow overview 115
BGP AS-Path 116
BGP Community 116
sFlow Datagram Flow 117
Configure sFlow forwarding on MPLS interfaces 118
Feature support matrix for sFlow 118
Configuring sFlow 119
Configuring sFlow globally 120
Enabling flow-based sFlow 120
Disabling flow-based sFlow on specific interfaces 121
Configuring sFlow for interfaces 121
sFlow agent address 123
Configuring Update Destination MAC in sFlow Streams for Routed Packets 124
Configuration example 124

Threshold Monitoring 127

Threshold Monitoring 127
Actions 127
Rate Limiting 128
Monitored Parameters 128
Configuring Message Rate Limiting Constraints for Threshold Monitoring 128
Configuring Threshold Monitor 129
MAC Collision Detection and Alarm 130

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a "soft" line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes

Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

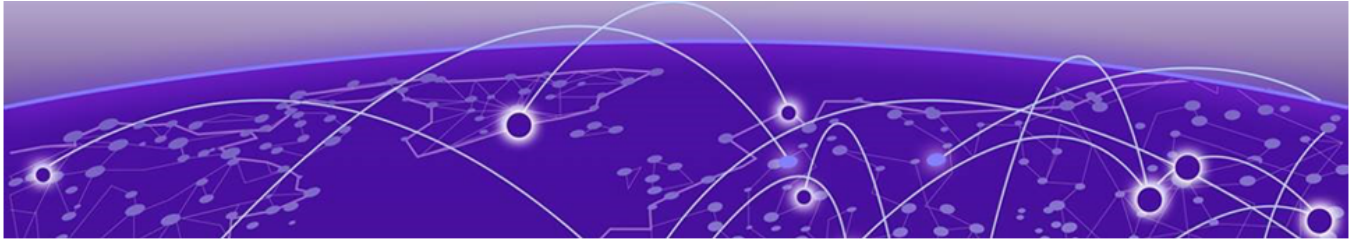
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About This Document

What's New in this Document on page 10
Supported Hardware on page 11
Regarding Ethernet interfaces and chassis devices on page 11

What's New in this Document

The following table includes descriptions of new information added to this document for the SLX-OS 20.7.3 software release.

Table 4: Changes made in Rev AB of this document

Field	Description	Described in
Optic Thresholds	In the topic *Optic Thresholds*, added a note clarifying the temperature range specified in the table is the operating temperature for the optic. Also added that the normal operating temperature range for the optic can be found in the https://optics.extremenetworks.com portal page for that optic.	Optic thresholds on page 77

Table 5: Changes made in Rev AA of this document

Feature	Description	Described in
Port Monitoring	Added a section in the topic *Hardware Monitoring* that describes how SLX-OS monitors Ports. This topic also describes the various I2C error types and how they are handled.	Port Monitoring on page 95
sFlow	In the topic *Feature support matrix for sFlow*, in the table titled *sFlow feature support*, added a row with information for *sFlow sampling over GRE tunnel*.	Feature support matrix for sFlow on page 118

For additional information, refer to the *Extreme SLX-OS Release Notes* for this version.

Supported Hardware

SLX-OS 20.7.3 supports the following hardware platforms.

- Extreme 8820
- Extreme 8720
- Extreme 8520
- ExtremeSwitching SLX 9540
- ExtremeSwitching SLX 9250
- ExtremeSwitching SLX 9150
- ExtremeRouting SLX 9740
- ExtremeRouting SLX 9640

Note

All configurations and software features that are applicable to SLX 9150 and SLX 9250 devices are also applicable for the Extreme 8520 and Extreme 8720 devices respectively.

All configurations and software features that are applicable to SLX 9740 devices are also applicable for the Extreme 8820 devices.

The "Measured Boot with Remote Attestation" feature is only applicable to the Extreme 8520, Extreme 8720, and Extreme 8820 devices. It is not supported on the SLX 9150 and SLX 9250 devices.

Note

Although many software and hardware configurations are tested and supported for this release, documenting all possible configurations and scenarios is beyond this document's scope.

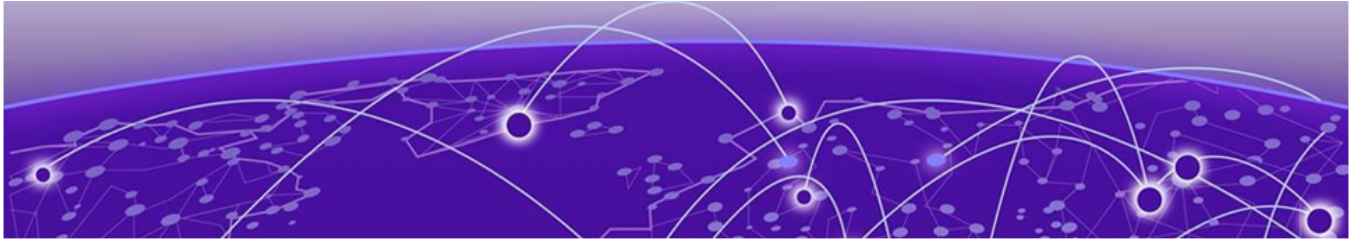
For information about other releases, see the documentation for those releases.

Regarding Ethernet interfaces and chassis devices

The current SLX-OS version does not support any multi-slot (chassis) devices.

However, the Ethernet interface configuration and output *slot/port* examples in this document may appear as either 0/x or n/x, where "n" and "x" are integers greater than 0.

For all currently supported devices, specify **0** for the slot number.



Operation, Administration, and Maintenance (OAM)

IEEE 802.1ag Connectivity Fault Management on page 12
Y.1731 Performance Monitoring on page 28
IEEE 802.3ah Ethernet in First Mile on page 42

IEEE 802.1ag Connectivity Fault Management

IEEE 802.1ag Connectivity Fault Management (CFM) refers to the ability of a network to monitor the health of a service delivered to customers as opposed to just links or individual bridges.

The IEEE 802.1ag CFM standard specifies protocols, procedures, and managed objects to support transport fault management. This allows for the discovery and verification of the path, through bridges and LANs, taken by frames addressed to and from specified network users and the detection, and isolation of a connectivity fault to a specific bridge or LAN.

Ethernet CFM defines proactive and diagnostic fault localization procedures for point-to-point and multipoint Ethernet Virtual Connections that span one or more links. It operates end-to-end within an Ethernet network.

Starting from SLX-OS 17r.2.00 release, CFM is supported over the virtual leased lines (VLL).

Y.1731 feature set support over VLL

Starting with the SLX-OS 17r.2.00 release, the Y.1731 feature set is supported over VLL. As shown in following figure, CFM or Y.1731 with UP MEPs can be configured for VLL.

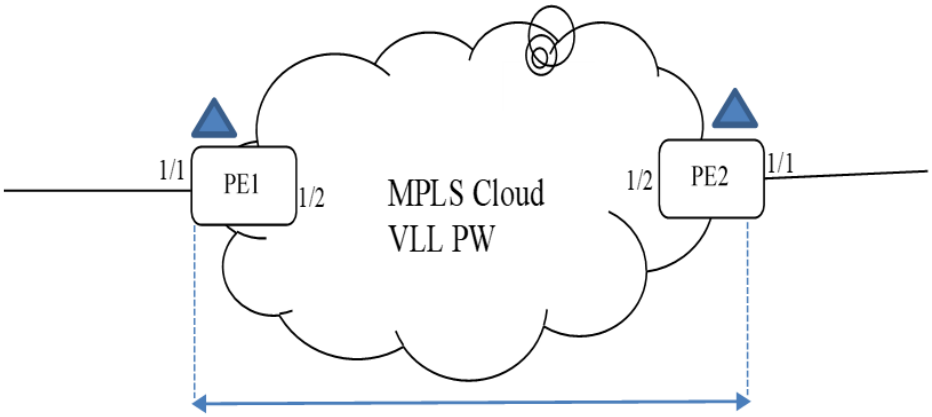


Figure 1: CFM UP MEP over VLL

The following figures show that CFM DOWM MEPs can be configured at the VLL Endpoint.

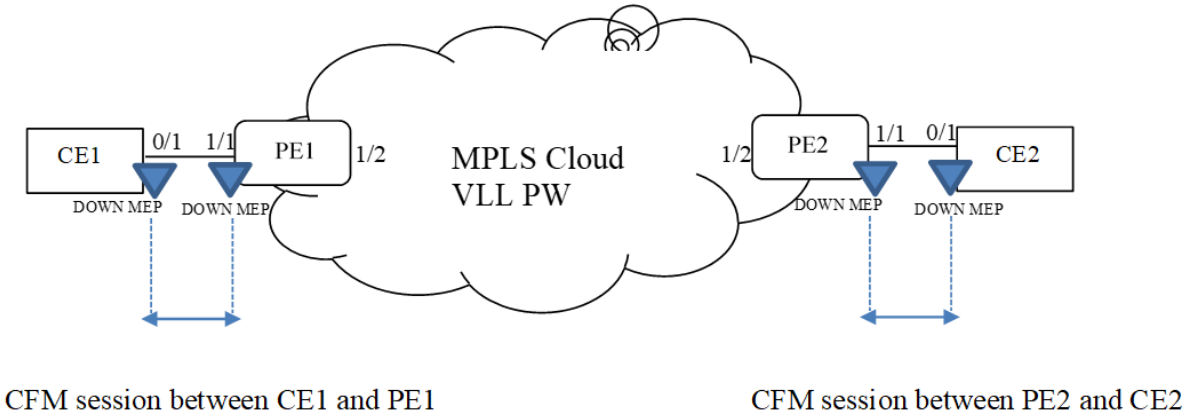


Figure 2: CFM DOWM MEP on VLL Endpoint

Ethernet OAM capabilities

Ethernet OAM is able to:

- Monitor the health of links (because providers and customers might not have access to the management layer)
- Check connectivity of ports
- Detect fabric failures
- Provide the building blocks for error localization tools
- Give appropriate scope to customers, providers and operators (hierarchical layering of OAM)
- Avoid security breaches

IEEE 802.1ag purpose

Bridges are increasingly used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM provides capabilities for detecting, verifying and isolating connectivity failures in such networks.

There are multiple organizations involved in a Metro Ethernet Service: Customers, Service Providers and Operators.

Customers purchase Ethernet Service from Service Providers. Service Providers may utilize their own networks, or the networks of other Operators to provide connectivity for the requested service. Customers themselves may be Service Providers, for example a Customer may be an Internet Service Provider which sells Internet connectivity.

Operators will need minimal Ethernet OAM. Providers will need more comprehensive Ethernet OAM for themselves and to allow customers better monitoring functionality.

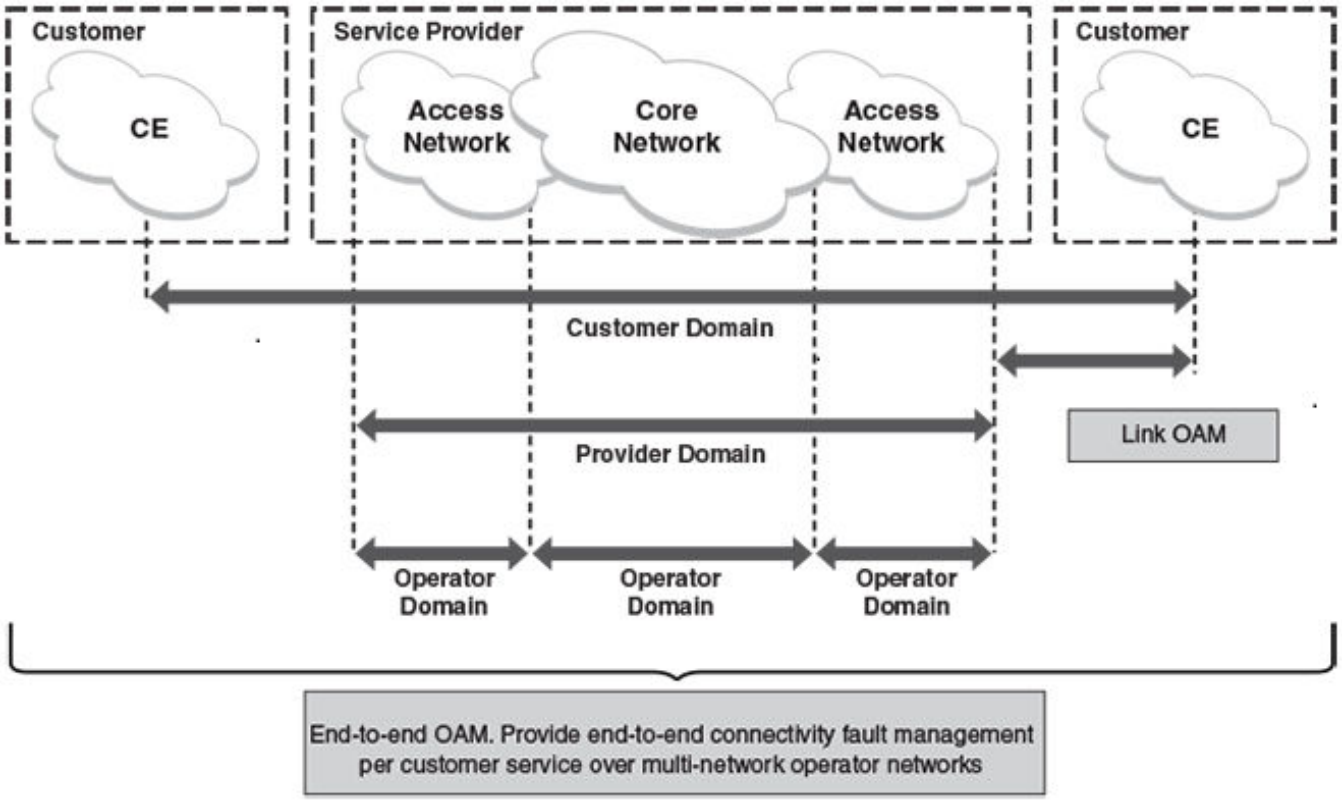


Figure 3: OAM Ethernet tools

IEEE 802.1ag hierarchical network management

Maintenance Domain

A Maintenance Domain (MD) is part of a network controlled by a single operator. Figure 3 on page 14, shows the customer domain, provider domain and operator domain.

Maintenance Domain level

The Maintenance Domain levels (MD level) are carried on all CFM frames to identify different domains. For example, in Figure 3 on page 14, some bridges belong to multiple domains. Each domain associates a MD level.

- Customer Level: 5-7
- Provider Level: 3-4
- Operator Level: 0-2

Maintenance Association

Every MD can be further divided into smaller networks having multiple Maintenance End Points (MEP). Usually a Maintenance Association (MA) is associated with service instances (for example a VLAN or a VPLS).

Maintenance End Point (MEP)

Maintenance End Point (MEP) is located on the edge of a Maintenance Association (MA). It defines the endpoint of the MA. Each MEP has unique ID (MEPID) within MA. The connectivity in a MA is defined as connectivity between MEPs. MEP generates Continuity Check Message and multicasts to all other MEPs in same MA to verify the connectivity.

Maintenance Intermediate Point

Maintenance Intermediate Point (MIP) is located within a Maintenance Association (MA). It responds to Loopback and Linktrace messages for Fault isolation.

Mechanisms of Ethernet IEEE 802.1ag OAM

Mechanisms supported by IEEE 802.1ag include Connectivity Check (CC), Loopback, and Link trace. Connectivity Fault Management allows end-to-end fault management that is generally reactive (through Loopback and Link trace messages) and connectivity verification that is proactive (through Connectivity Check messages).

Fault detection (Continuity Check Message)

The Continuity Check Message (CCM) provides a means to detect hard and soft faults such as software failure, memory corruption, or misconfiguration. The failure detection is achieved by each Maintenance End Point (MEP) transmitting a CCM periodically within its associated Service Instance.

As a result, MEPs also receive CCMs periodically from other MEPs. If a MEP on local Bridge stops receiving the periodic CCMs from peer MEP on a remote Bridge, it can assume that either the remote Bridge has failed or failure in the continuity of the path has occurred. The Bridge can subsequently notify the network management application about the failure and initiate the fault verification and fault isolation steps either automatically or through operator command.

A CCM requires only N transmissions within its member group, where N is the number of members within the member group. In other words, if a Virtual Bridge LAN Service has N members, only N CCMs need to be transmitted periodically, one from each.

Each MEP transmits periodic multicast CCM towards other MEPs. For each MEP, there is 1 transmission and N-1 receptions per time period. Each MEP has remote MEP database. It records the Mac address of remote MEPs.

Continuity Check (CC) messages are periodic hello messages multicast by a MEP within the maintenance domain, at the rate of X; X can be 3 milliseconds (ms), 10ms, 100ms, 1 second or 10 seconds. All Maintenance association Intermediate Points (MIPs) and MEPs in that domain will receive it but will not respond to it. The receiving MEPs will build a MEP database that has entities of the format. MEPs receiving this CC message will catalog it and know that the various maintenance associations (MAs) are functional, including all intermediate MIPs.

CCMs are not directed towards any specific; rather they are multicast across the entire point-to- point or multipoint service on a regular basis. Accordingly, one or more service flows, including the determination of MAC address reachability across a multipoint network, are monitored for connectivity status with IEEE 802.1ag.

Fault verification (Loopback messages)

A unicast Loopback Message is used for fault verification. To verify the connectivity between MEP and its peer MEP or a MIP, the Loopback Message is initiated by a MEP with a destination MAC address set to the MAC address of either a Maintenance association Intermediate Point (MIP) or the peer MEP. The receiving MIP or MEP responds to the Loopback Message with a Loopback Reply.

A Loopback message helps a MEP identify the precise fault location along a given MA. A Loopback message is issued by a MEP to a given MIP along an MA. The appropriate MIP in front of the fault will respond with a Loopback reply. The MIP behind the fault will not respond. For Loopback to work, the MEP must know the MAC address of the MIP to ping.

Fault isolation (Linktrace messages)

Linktrace mechanism is used to isolate faults at Ethernet MAC layer. Linktrace can be used to isolate a fault associated with a given Virtual Bridge LAN Service. It should be noted that fault isolation in a connectionless (multi-point) environment is more challenging than a connection oriented (point-to-point) environment. In case of Ethernet, fault isolation can be even more challenging since a MAC address can age out when a fault isolates the MAC address. Consequently a network-isolating fault results in erasure of information needed for locating the fault.

A Linktrace Message uses a set of reserved multicast MAC address. The Linktrace Message gets initiated by a MEP and traverses hop-by-hop and each Maintenance Point (a MEP or MIP) along the path intercepts this Linktrace Message and forwards it onto the next hop after processing it until it reaches the destination MEP. The processing includes looking at the destination MAC address contained in the Linktrace Message.

Each MP along the path returns a unicast Linktrace Reply back to the originating MEP. The MEP sends a single LTM to the next hop along the trace path; however, it can receive many Linktrace Responses from different MPs along the trace path and the destination MEP as the result of the message traversing hop by hop. As mentioned previously, the age-out of MAC

addresses can lead to erasure of information at MIPs, where this information is used for the Linktrace mechanism. Possible ways to address this behavior include:

- Carrying out Linktrace following fault detection or verification such that it gets exercised within the window of age-out.
- Maintaining information about the destination MEP at the MIPs along the path using CCMs.
- Maintaining visibility of path at the source MEPs through periodic LTMs.

Linktrace may also be used when no faults are apparent in order to discover the routes normally taken by data through the network. In the rare instances during network malfunctions where Linktrace cannot provide the information needed to isolate a fault, issuing Loopback Messages to MPs along the normal data path may provide additional useful information.

The Linktrace message is used by one MEP to trace the path to another MEP or MIP in the same domain. It is needed for Loopback (Ping). All intermediate MIPs respond back with a Link trace reply to the originating MEP. After decreasing the TTL by one, intermediate MIPs forward the Link trace message until the destination MIP or MEP is reached. If the destination is a MEP, every MIP along a given MA responds to the originating MEP. The originating MEP can then determine the MAC address of all MIPs along the MA and their precise location with respect to the originating MEP.

802.1ag Connectivity Fault Management

Bridges are increasingly used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM provides capabilities for detecting, verifying and isolating connectivity failures in such networks.

There are multiple organizations involved in a Metro Ethernet Service: Customers, Service Providers and Operators.

Customers purchase Ethernet Service from Service Providers. Service Providers may utilize their own networks, or the networks of other Operators to provide connectivity for the requested service. Customers themselves may be Service Providers, for example a Customer may be an Internet Service Provider which sells Internet connectivity.

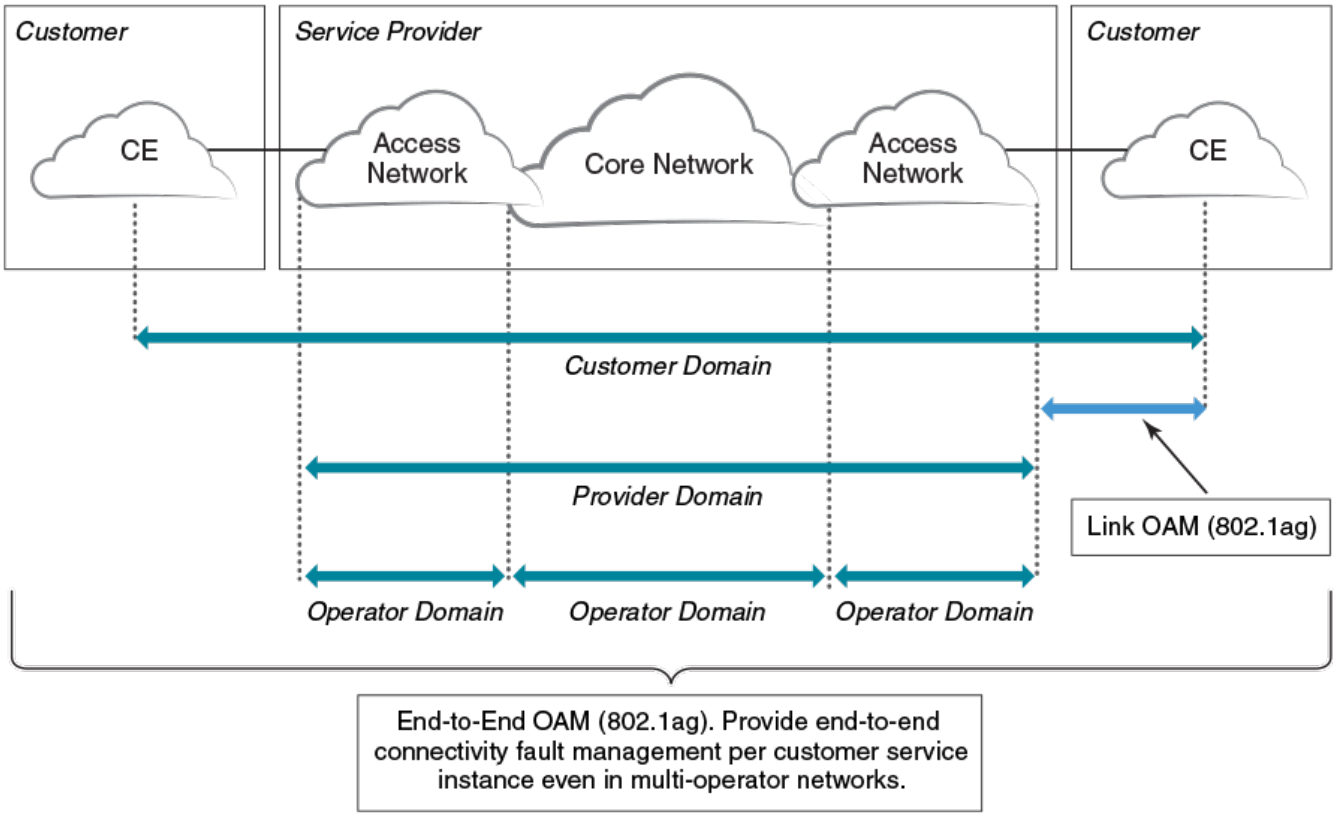


Figure 4: OAM Ethernet tools

Maintenance Domain (MD)

A Maintenance Domain is part of a network controlled by a single operator. In the following figure, a customer domain, provider domain and operator domain are described.

The Maintenance Domain (MD) levels are carried on all CFM frames to identify different domains. For example, in the following figure, some bridges belong to multiple domains. Each domain associates to an MD level.

- Customer Level: 5-7
- Provider Level: 3-4
- Operator Level: 0-2

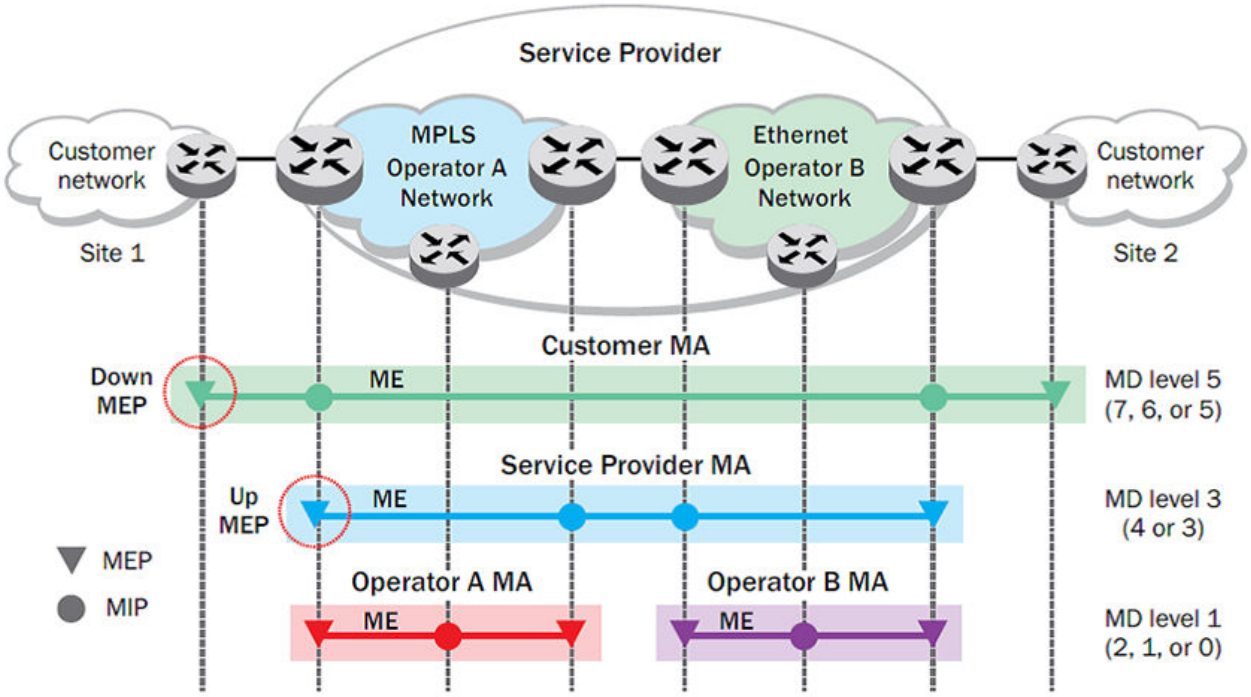


Figure 5: CFM deployment

Maintenance Association (MA)

Every MD can be further divided into smaller networks having multiple Maintenance End Points (MEP). Usually an MA is associated with a service instance (for example, a VLAN or a VPLS).

Maintenance End Point (MEP)

An MEP is located on the edge of an MA and defines the endpoint of the MA. Each MEP has unique ID (MEPID) within the MA. The connectivity in a MA is defined as connectivity between MEPs. MEPs generate a Continuity Check Messages that are multicast to all other MEPs in same MA to verify the connectivity.

Each MEP has a direction, down or up. Down MEPs receive CFM PDUs from the LAN and sends CFM PDUs towards the LAN. Up MEPs receive CFM PDUs from a bridge relay entity and sends CFM PDUs towards the bridge relay entity on a bridge. End stations support down MEPs only, as they have no bridge relay entities.

Maintenance Intermediate Point (MIP)

An MIP is located within a MA. It responds to Loopback and Linktrace messages for Fault isolation.

CFM Hierarchy

MD levels create a hierarchy in which 802.1ag messages sent by customer, service provider, and operators are processed by MIPs and MEPs at the respective level of the message. A common practice is for the service provider to set up a MIP at the customer MD level at the edge of the network, as shown in the figure above, to allow the customer to check continuity

of the Ethernet service to the edge of the network. Similarly, operators set up MIPs at the service provider level at the edge of their respective networks, as shown in the figure above, to allow service providers to check the continuity of the Ethernet service to the edge of the operators' networks. Inside an operator network, all MIPs are at the respective operator level, also shown in the figure above.

Mechanisms of Ethernet IEEE 802.1ag OAM

Mechanisms supported by IEEE 802.1ag include Connectivity Check (CC), Loopback, and Link trace. Connectivity Fault Management allows for end-to-end fault management that is generally reactive (through Loopback and Link trace messages) and connectivity verification that is proactive (through Connectivity Check messages).

Fault detection (continuity check message)

Each MEP transmits periodic multicast CCMs towards other MEPs. For each MEP, there is 1 transmission and n-1 receptions per time period. Each MEP has a remote MEP database. It records the MAC address of remote MEPs.

Fault verification (Loopback messages)

A unicast Loopback Message is used for fault verification. A Loopback message helps a MEP identify the precise fault location along a given MA. A Loopback message is issued by a MEP to a given MIP along an MA. The appropriate MIP in front of the fault responds with a Loopback reply. The MIP behind the fault do not respond. For Loopback to work, the MEP must know the MAC address of the MIP to ping.

Fault isolation (Linktrace messages)

Linktrace mechanism is used to isolate faults at Ethernet MAC layer. Linktrace can be used to isolate a fault associated with a given Virtual Bridge LAN Service. Note that fault isolation in a connectionless (multi-point) environment is more challenging than a connection oriented (point-to-point) environment. In case of Ethernet, fault isolation can be even more challenging since a MAC address can age out when a fault isolates the MAC address. Consequently a network-isolating fault results in erasure of information needed for locating the fault.

Enabling or disabling CFM

To enable or disable the Connectivity Fault Management (CFM) protocol globally on the devices and enter into the CFM protocol configuration mode, enter the following command.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)#
```

The **no** form of the command disables the CFM protocol.

Creating a Maintenance Domain

A Maintenance Domain (MD) is the network or the part of the network for which faults in connectivity are to be managed. A Maintenance Domain consists of a set of Domain Service Access Points.

An MD is fully connected internally. A Domain Service Access Point associated with an MD has connectivity to every other Domain Service Access Point in the MD, in the absence of faults.

Each MD can be separately administered.

The **domain-name** command in Connectivity Fault Management (CFM) protocol configuration mode creates a maintenance domain with a specified level, name, and ID and enters the specific MD mode specified in the command argument.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 id 1 level 4
device(config-cfm-md-md1)#
```

The **no** form of the command removes the specified domain from the CFM protocol configuration mode.

Creating and configuring a Maintenance Association

1. Create a MA within a specific domain, use the **ma-name** command.

   ```
   device# configure terminal
   device(config)# protocol cfm
   device(config-cfm)# domain name md1 id 1 level 4
   device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 4
   device(config-cfm-md-ma-ma1)#
   ```

   This command changes the Maintenance Domain (MD) mode to the specific MA mode.
2. Set the time interval between two successive Continuity Check Messages (CCMs) that are sent by Maintenance End Points (MEP) in the specified MA, use the **ccm-interval** command.

   ```
   device# configure terminal
   device(config)# protocol cfm
   device(config-cfm)# domain name md1 id 1  level 4
   device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
   device(config-cfm-md-ma-ma1)# ccm-interval 10-second
   device(config-cfm-md-ma-ma1)#
   ```

   The id field specifies the short MAID format that is carried in the CCM frame. The default time interval is 10 seconds.
3. Add local ports as MEP to a specific maintenance association using the **mep** command in MA mode.

   ```
   device# configure terminal
   device(config)# protocol cfm
   device(config-cfm)# domain name md1 id 1 level 4
   device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
   device(config-cfm-md-ma-ma1)# mep 1 down ethernet 1/2
   device(config-cfm-md-ma-mep-1)#
   ```

   To configure a CFM packet to a Down MEP, you must sent it out on the port on which it was configured. To configure a Connectivity Fault Management (CFM) packet to an Up MEP, you must sent it to the entire VLAN for multicast traffic and the unicast traffic must be sent to a particular port as per the MAC table.
4. Configure the remote MEPs using the **remote-mep** command.

   ```
   device# configure terminal
   device(config)# protocol cfm
   device(config-cfm)# domain name md1 id 1clevel 4
   device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
   device(config-cfm-md-ma-ma1)# mep 1 down ethernet 1/2
   ```

```
device(config-cfm-md-ma-mep-1)# remote-mep 2
device(config-cfm-md-ma-mep-1)#
```

If a remote MEP is not specified, the remote MEP database is built based on the CCM. If one remote MEP never sends CCM, the failure cannot be detected.

5. Configure the conditions to automatically create MIPs on ports using the **mip-policy** command, in Maintenance Association mode.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 id 1 level 4
device(config-cfm-md-md1)#ma-name ma1 id 1 vlan-id 30 pri 7
device(config-cfm-md-ma-ma1)#mip-policy explicit
device(config-cfm-md-ma-ma1)#
```

A MIP can be created on a port and VLAN, only when explicit or default policy is defined for them. For a specific port and VLAN, a MIP is created at the lowest level. Additionally, the level created should be the immediate higher level than the MEP level defined for this port and VLAN.

Displaying CFM configurations

The following commands are used to display the CFM configurations and connectivity status.

show cfm

Use the **show cfm** command to display the Connectivity Fault Management (CFM) configuration.

```
device# show cfm
Domain: md1
Index: 1
Level: 7
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
  MEP   Direction  MAC              PORT       VLAN         INNER-VLAN   PORT-STATUS-TLV
  ====  =========  =========        ====       ====         ===========  ===============
  1     UP         609c.9f5f.700d   Eth 1/9    50           --           N
```

Note
For the **show cfm** command to generate output, you must first enable CFM in protocol configuration mode.

show cfm connectivity

Use the **show cfm connectivity** command to display the Connectivity Fault Management (CFM) configuration.

The following commands display the received port status tlv state at RMEP.

```
device# show cfm connectivity
Domain: md1
Index: 1
Level: 7
  Maintenance association: ma5
  MA Index: 5
```

```
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
    MEP Id: 1
    MEP Port: Eth 1/9
      RMEP  MAC             VLAN/PEER         INNER-VLAN    PORT      STATE
      ====  ===             =========         ==========    ====      =====
      2     609c.9f5e.4809  19.1.1.1           --            --       OK
```



Note
For the **show cfm** command to generate output, you must first enable CFM in protocol configuration mode.

show cfm brief

Use the **`show cfm brief`** command to display the Connectivity Fault Management (CFM) brief output.

```
device# show cfm brief
Domain: md1
Index: 1
Level: 7  Num of MA: 1
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
  Num of MEP: 1  Num of RMEP: 1
  rmepfail: 0 rmepok: 1
```

CFM over double tagged end-points

Domain double-tagged support for CFM enables up and down MEP at a double-tagged provider edge. For a Bridge Domain double tagged port to advertise CFM, the CLI command must specify the inner VLAN while configuring the MEP using the **mep** command as follows.

For more information on the command, please refer the SLX-OS Command Reference guide.

The **show cfm** command displays the inner vlan-id for MEP as follows.

```
device# show cfm
Domain: dom1
Level: 5
  Maintenance association: ma1
  MA Index: 4
  CCM interval: 10000 ms
  Bridge-Domain ID: 100
  Priority: 4
  MEP   Direction  MAC              PORT        VLAN     PORT-STATUS-TLV
  ====  =========  =========        ====        =======  ===============
  11    DOWN       768e.f80a.9903   Eth 2/15    100,200       N
```

The **show cfm connectivity** command displays the inner vlan-id for the remote MEP as follows.

```
SLX# show cfm connectivity
Domain: dom1
Level: 5
  Maintenance association: ma1
  MA Index: 4
  CCM interval: 10000
  Bridge-Domain ID: 100
  Priority: 4
  MAID Format: Short
    MEP Id: 2
    MEP Port: Eth 1/5
      RMEP     MAC                    VLAN/PEER            PORT         STATE
      ====      ===                    =========             ====          =====
      3          0010.9400.0002        100,200               Eth 1/5        OK
```

Monitoring the status of devices in a VPLS network in a Provider's Maintenance Domain

CFM provides capabilities to detect, verify, and isolate connectivity failures.

Note
When configuring 802.1ag over VPLS, if the VPLS endpoint is deleted from the configuration, the MEP configuration is deleted under CFM without warning.

In the following figure, CFM is applied over a VPLS network; ports 1/2 and 1/3 are customer facing networks; and port 1/1 is an uplink to a VPLS cloud.

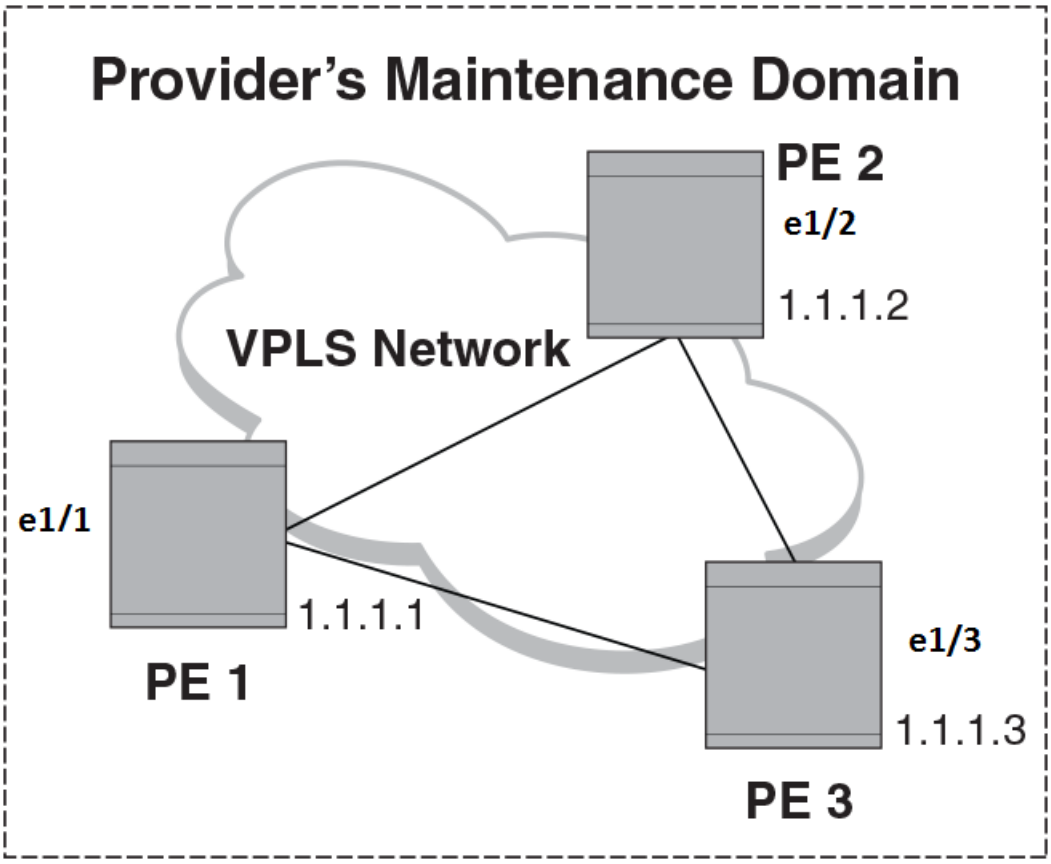


Figure 6: VPLS cloud with CFM enabled

Configuring PE

1. To enable CFM for VPLS, enter the following command.

```
device(config)# protocol cfm
device(config-cfm)#
```

2. Create a maintenance domain with a specified name and level.

```
device(config-cfm)# domain-name md1 id 1 level 7
device (config-cfm-md-md1)#
```

3. Create a maintenance association for the VPLS service.

```
device (config-cfm-md-md1)# ma ma1 id 5 bridge-domain 20 priority 7
device (config-cfm-md-ma-ma1)#
```

4. Create an MEP for the VPLS service.

```
device(config-cfm-md-ma-ma1)# mep 101 down vlan 100 ethernet 1/2
device(config-cfm-md-ma-mep-101)#
```

Note
Follow the same steps to configure PE2 and PE3, to complete the configuration shown in Figure 2. All CFM configuration is same in PE2 and PE3 except the mep-id, which is configured with a different values on PE2 and PE3.

VPLS configurations

Enter the following commands to configure VPLS peers from PE 2 to PE3.

1. From the configuration mode, configure virtual ethernet interface in trunk mode using the **`switchport mode`** command.

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no ip address
device(conf-if-eth-1/1)# switch port mode trunk
```

2. Configure a logical interface using the **`logical-interface`** command.

```
device(conf-if-eth-1/1)# logical-interface eth 1/1.20
device(conf-if-eth-lif-1/1.20)
```

3. Configure VLAN on the logical interface.

```
device(conf-if-eth-lif-1/1.20)# vlan 100
```

4. Turn on the interface using the **`no shutdown`** command.

```
device(conf-if-eth-lif-1/1.20)# exit
device(conf-if-eth-1/1)# no shutdown
```

5. From the global configuration mode, create a bridge domain using the **`bridge-domain`** command and configure peers.

```
device(conf-if-eth-1/1)# exit
device(config)# bridge-domain 100
device(config-bridge-domain-100)# vc-id 20
device(config-bridge-domain-100)# peer 1.1.1.2
device(config-bridge-domain-100)# peer 1.1.1.3
```

6. Enter **`no bpdu-drop-enable`** command to disable BPDU drop.

```
device(config-bridge-domain-100)# no bpdu-drop-enable
```

7. Verify the running configuration.

```
device(config-bridge-domain-100)# do show run br

bridge-domain 100 p2mp
vc-id 20
peer 1.1.1.2
peer 1.1.1.3
logical-interface ethernet 1/1.20
pw-profile default
local-switching
!
device(config-bridge-domain-100)#
```

Tracing the network path using IEEE 802.1ag Linktrace

You can manually monitor the status of peers using IEEE 802.1ag **`CFM Linktrace`** commands. LTM message is generated when link trace is performed.

```
device# cfm linktrace domain md1 ma ma1 src-mep 101 target-mep 200
```

Following are the parameters which you can configure for the **CFM Linktrace** command.

- The **domain** *name* parameter specifies the maintenance domain to be used for a linktrace message. The *name* attribute is case-sensitive.
- The **ma** *ma-name* parameter specifies the maintenance association to be used for a linktrace message. The *name* attribute is case-sensitive.
- The **src-mep** *mep-id* parameter specifies the Source ID in the range 1-8191.
- The **target-mip** *HHHH.HHHH.HHHH.HHHH* parameter specifies the MAC-address of the MIP linktrace destination.
- The **target-mep** *mepid* parameter specifies the ID of the linktrace destination.
- The **timeout** *timeout* parameter specifies the timeout used to wait for linktrace reply and the value range from 1-30 seconds.
- The **ttl** *TTL* parameter specifies the initial TTL field value in the range 1-64. The default value is 8.

Verifying connectivity using IEEE 802.1ag Loopback

```
device# cfm loopback domain md1 ma ma1 src-mep 101 target-mep 200
```

Following are the parameters which you can configure for the **CFM loopback domain** command.

- The **domain** *name* parameter specifies the maintenance domain to be used for a loopback message. The *name* attribute is case-sensitive.
- The **ma** *ma-name* parameter specifies the maintenance association to be used for a loopback message. The *ma-name* attribute is case-sensitive.
- The **src-mep** *mep-id* parameter specifies the Source ID in the range 1-8191.
- The **target- mip** *HHHH:HHHH:HHHH* parameter specifies the MAC address of the MIP loopback destination.
- The **target-mep** *mep-id* parameter specifies the Destination ID in the range 1-8191.
- The **number** *number* parameter specifies the number of loopback messages to be sent.
- The **timeout** *timeout* parameter specifies the timeout used to wait for loopback reply.

Syslog message

If CFM is configured, a syslog message will be generated when remote MEPs change their states or if there are service cross connections.

Sample Syslog Messages

```
device#
SYSLOG: 2016/08/11-21:46:15,[EOAM-1002], 3217, M1 | Active | DCE, INFO, SLX, DOT1AG :
Remote MEP 2 in Domain md1, MA ma1 become UP state.
SYSLOG: 2016/08/11-21:46:50, [EOAM-1003], 3218, M1 | Active | DCE, INFO, SLX, DOT1AG :
Remote MEP 2 in Domain md1, MA ma1 aged out.
```

Scale

A total of 4000 MEP sessions and 8000 RMEP sessions can be configured in the system. Note that this scale is applicable overall for the system. You can configure all of the above-mentioned MEP session and RMEP sessions on a single port.

Y.1731 Performance Monitoring

About Y.1731 Performance Monitoring

The Y.1731 feature provides the following performance monitoring capability for point-to-point links as defined in ITU-T Rec Y.1731. The following Y.1731 features are supported in the current release.

- Two-Way ETH-SLM
- Two-Way ETH-DM

Y.1731 defines the following parameters and functions for performance monitoring.

Frame Loss Ratio—The Frame loss ratio is defined as a ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T, where the number of service frames not delivered is the difference between the number of service frames arriving at the ingress ETH flow point and the number of service frames delivered at the egress ETH flow point in a point-to-point ETH connection.

Frame Delay— Frame delay can be specified as round-trip delay for a frame, where Frame Delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the loop backed frame by the same source node, when the loopback is performed at the frame's destination node.

Frame Delay Variation— Frame delay variation is a measure of the variations in the Frame Delay between a pair of service frames, where the service frames belong to the same CoS instance on a point-to-point ETH connection.

Y.1731 features not supported in SLX-OS

Extreme SLX-OS software does not support the following Y.1731 features:

- Frame Loss Measurement (ETH-LMM)
- One Way Delay Measurement (One-way ETH-DM)
- One Way Synthetic Loss Measurement (One-way ETH-SLM)
- Throughput measurement
- AIS and RDI
- Y.1731 over point to multi-point (P2MP) and multi-point to multi-point (MP2MP) ETH connections

Y.1731 support in SLX-OS Hardware

Y.1731 is supported in the following SLX-OS devices:

- SLX 9540
- SLX 9640

Limitations and Restrictions

- Maximum value of frame_delay can be 4 seconds. If a frame delay response packet is received after the delay, the packet is discarded and frame_delay calculation for that packet cannot be performed.
- Only one action profile can be attached to a source MEP and remote MEP (RMEP) pair.

Note
We recommend that you issue the **`linktrace`** command before configuring on-demand Two-way ETH-DM or Two-way ETH-SLM to know the forwarding path.

Two-way ETH-SLM and Two-way ETH-DM

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 belonging to the same domain and MA.

Synthetic loss measurement is a mechanism to measure frame loss using synthetic frames, rather than data traffic. A number of synthetic frames are sent and received, and the number of those that are lost is hence calculated to measure the loss.

Note
A MIP is transparent to the frames with ETH-SLM information and therefore does not require any information to support the ETH-SLM functionality.

Two-Way ETH-SLM

In a Two-Way ETH-SLM, Initiator (the source MEP) sends burst of Synthetic Loss Message (SLM) frames to Responder (the Remote MEP) and in turn receives Synthetic Loss Reply (SLR) frames to carry out synthetic loss measurements.

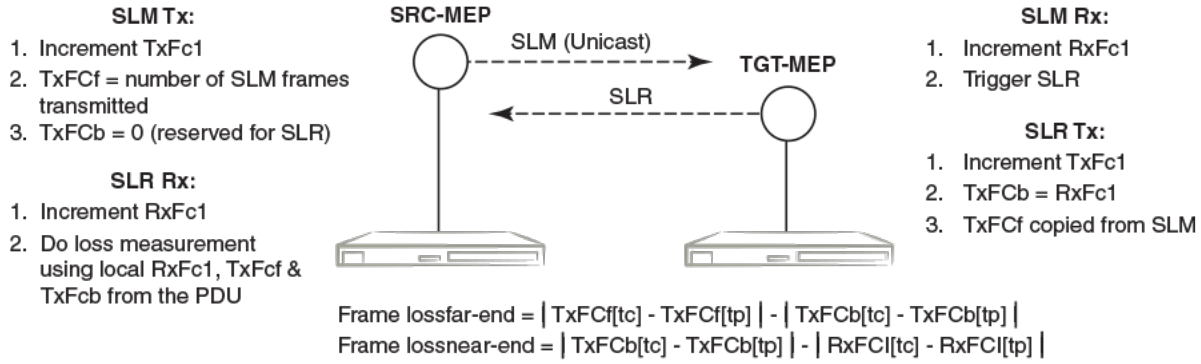


Figure 7: Two-Way ETH-SLM

A MEP transmits burst of SLM frames once for every Tx-interval time period. Whenever a valid SLM frame is received by a MEP, an SLR frame is generated and transmitted to the initiating MEP. With the information contained in SLR frames, a MEP determines frame loss for given measurement periods.

Loss measurement calculation

For each MA where Two-Way ETH-SLM is configured, an MEP maintains two local counters for each peer MEP for each CoS instance which plays a role in calculating Loss Measurement.

TxFC1: Counter for synthetic frames transmitted towards the peer MEP. A source MEP increments this counter with transmission of SLM frames while a responder MEP increments it with transmission of SLR frames.

RxFC1: Counter for synthetic frames received from the peer MEP. A source MEP increments this counter with reception of SLR frames while a responder MEP increments it with reception of SLM frames.

A MEP uses the following values to determine near-end and far-end frame loss in the measurement period:

- Last received SLR frame's TxFCf and TxFCb values and local counter RxFCl at the end of the measurement period. These values are represented as TxFCf[tc], TxFCb[tc] and RxFCl[tc], where tc is the end time of the measurement period.
- SLR frame's TxFCf and TxFCb values of the first received SLR frame after the test starts and local counter RxFCl at the beginning of the measurement period. These values are represented as TxFCf[tp], TxFCb[tp] and RxFCl[tp], where tp is the start time of the measurement period.

Frame lossfar-end = | TxFCf[tc] – TxFCf[tp] | – | TxFCb[tc] – TxFCb[tp] |

Frame lossnear-end = | TxFCb[tc] – TxFCb[tp] | – | RxFCl[tc] – RxFCl[tp] |

On-demand SLM

The following points applies to On-demand SLM.

- SLR frames received after the timeout interval are discarded.
- SLM frames are sent in a burst.
- The maximum tx-frame-count per session is 300.
- If an on-demand session is initiated with a profile having tx-frame-count greater than 300, the device sends only 300 packets.

Delay Measurement

The ETH-DM is used for on-demand OAM to measure frame delay and frame delay variation.

Frame delay and frame delay variation measurements are performed by sending frames with ETH-DM information to the peer MEP and receiving frames with ETH-DM information during the diagnostic interval. Each MEP performs the frame delay and frame delay variation measurement.

For the MEP to support ETH-DM, you must configure the following.

- MEG (or MA) Level— MEG (or MA) Level at which the MEP exists.
- Priority— Identifies the priority of the frames with ETH-DM information.

Two-way ETH-DM

In a Two-way ETH-DM, an Initiator or a Source MEP sends frames with ETH-DM request information (DMM) to the Responder or a Remote MEP and in turn receives frames with ETH-DM reply information (DMR) to carry out two-way frame delay and two-way frame delay variation measurements.

Delay measurement calculation

When delay measurement is issued, a MEP transmits DMM frames with the 'TxTimeStampf' value.

When a valid DMM frame is received by a MEP, a DMR frame is generated and transmitted to the requesting MEP. A DMM frame with a valid domain level and a destination MAC address equal to the receiving MEP's MAC address is considered as a valid DMM frame. There are two additional timestamps which are used in the DMR frame to take into account the processing time at the remote MEP: 'RxTimeStampf' (Timestamp at the time of receiving the DMM frame) and 'TxTimeStampb' (Timestamp at the time of transmitting the DMR frame).

After receiving a DMR frame, a MEP tags the incoming frame with another timestamp 'RxTimeStampb' and uses the following values to calculate two-way frame delay.

Frame Delay = (RxTimeStampb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)

The MEP can also make two-way frame delay variation measurements based on its capability to calculate the difference between two subsequent two-way frame delay measurements.

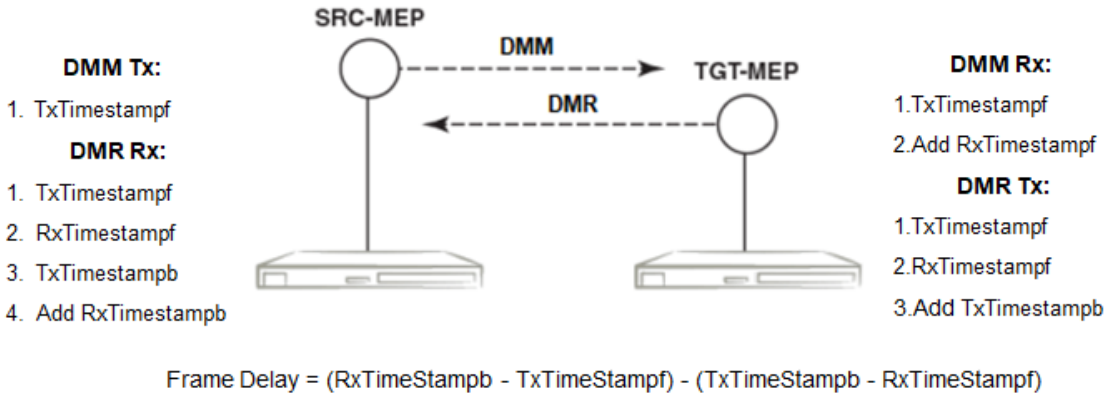


Figure 8: Two-Way ETH-DM

Test Profile

SLX-OS provides the default test profile, configurable test profile and configurable action profile that can be associated to a source and target MEP pair at the initiator or responder side which establishes a session. This facilitates the user to apply all the parameters which are configured within the profile at once for a measurement session instead of specifying each parameter through the command-line interface (CLI).

The following table provides information on the two important counters used for loss measurement.

	Initiator	Responder
TxFC1	SLM Tx count	SLR Tx count
RxFC1	SLR Rx count	SLM Rx count

- **Default test profile**: A default test profile for either Two-way ETH-DM or Two-way ETH-SLM session can be directly associated to a source and target MEP pair with default values of the required parameters to start the measurement.

Table 6: Default Two-way ETH-DM Test Profile

Parameter	Default value
Name	2dm-default-profile
CoS	7
tx Interval	1 second
Measurement Interval	15 minutes
Threshold average	4294967295 uSec
Threshold Max	4294967295 uSec
Start Time	00:05:00 (After)
Stop Time	01:05:00 (After)
Number of packets	10
Timeout	1 second

Table 7: Default Two-way ETH-SLM Test Profile

Parameter	Default Value
Name	2slm-default-profile
CoS	7
tx Interval	1 second
Measurement Interval	15 minutes
Threshold Backward Average	4294967295 milliPercent
Threshold Backward Max	4294967295 milliPercent
Threshold Forward Average	4294967295 milliPercent
Threshold Forward Max	4294967295 milliPercent
Start Time	00:05:00 (After)
Stop Time	01:05:00 (After)
Number of packets	10
Timeout	1 second

The default test profile can be associated with an on-demand session or a scheduled (or periodic) session.

Note
Default profiles can neither be updated nor be deleted.

Note
For a scheduled session associated with a default profile, the start time can be 5 minutes and the stop time can be 1 hr 5 minutes from the time a session is configured that is for a total duration of one hour with measurement interval of 15 minutes.

Note
Note: The threshold values in the default profile are set to MAX value and hence this cannot trigger Syslogs, SNMP Traps or any action if configured in action profile for the threshold parameter.

- **Test profile**: You can configure a test profile with custom values for each parameter either for an on-demand or scheduled (or periodic) Two-way ETH-DM or Two-way ETH-SLM session. You can specify if the measurement type is a Two-way ETH-DM or Two-way ETH-SLM session while configuring the test profile.

  Note
  Tx-interval, measurement interval and threshold are applicable for only initiator and not for responder.

  Note
  Start time, stop time and Tx-interval parameter default values are not applicable for an on-demand session.

  Note
  For Two-way ETH-SLM sessions, the noumber of packets specified are sent in a burst at once for On Demand sessions and for every Tx-interval for Scheduled sessions. The timeout is applicable for the entire burst of frames for On-demand sessions.

  For Two-way ETH-DM sessions, the packets are sent sequentially after every reply message received for On-demand for a total number of packets specified and for every Tx-interval

for scheduled (or periodic) sessions. The timeout is applicable per packet only for On-demand sessions.

Note
The configured test profile determines the type of Y.1731 measurement feature and the CLI used for initiating the measurement session is generic for both ETH-DM and ETH-SLM.

Note
If a profile is updated which is already associated to an active Two-way ETH-DM or Two-way ETH-SLM session, the current active session(s) will be implicitly stopped before the profile is updated. The updated profile would be applicable for the next scheduled (or periodic) session(s). However as an exception, if the stop time in the profile associated with an active session is updated to a later time than the current time, the session(s) will not be stopped and the new configured stop time in the profile will be applied immediately.

For an on-demand active session, there will be no impact of such updating of the associated profile.

- **Action profile**: You can configure an action profile with options to specify which action has to be taken when a configured event is encountered.

  The configurable events are as follows:
  - Average Threshold
  - Max Threshold
  - CCM Down
  - CCM Up

  The configurable actions are as follows:
  - Interface Down
  - Event Handler
  - All

  For all these events, syslog is the default action.

  Note
  One action profile can have multiple event-action associations contained in it. The threshold values in the default profile are set to MAX value and hence this cannot trigger Syslog or any action, if configured in action profile for the threshold parameter.

  Note
  The threshold events configured in an action profile can be triggered during an on-demand or a scheduled (or periodic) Two-way ETH-DM or Two-way ETH-SLM sessions.

Configuration considerations

An MEP instance must be configured before configuring ETH-SLM or ETH-DM.

- An MEP instance must be configured before configuring ETH-SLM or ETH-DM.
- The configured test profile determines the type of Y.1731 measurement feature and the command line interface (CLI) used for initiating the measurement session is generic for all supported Y.1731 measurement features.
- A ETH-DM or ETH-SLM scheduled session cannot be started if the Remote MEP is not learnt. However, the session can start if the remote MEP is known but in a failed state.
- Link Down or/and RMEP age out will not stop any active Two-way ETH-SLM or Two-way ETH-DM session but will be considered as frame loss.
- Before initiating a Scheduled Two-Way ETH-DM or Two-Way ETH-SLM session, the responder need to be configured prior to the initiator.
- A session run with CoS value of 8 specifies that a random CoS value between 0 and 7 would be applied to the session and hence no other session with other CoS values can be started for that RMEP and vice-versa in this scenario, i.e. If a session is already running with CoS value of (0 to 7) on this RMEP, a session with CoS value of 8 cannot be started and error will be thrown to user in both scenarios.
- History data generated after every measurement cycle for a scheduled ETH-DM or ETH-SLM session overwrites the oldest entry after 32 history entries.
- The 'Tx-interval', 'measurement-interval' and 'Threshold' values in a default or configured test profile are applicable for only initiator and not for responder.
- The 'Start time', 'Stop time' and 'Tx-interval' parameter values in a default or configured test profile are not applicable for an on-demand ETH-DM or ETH-SLM sessions.
- For ETH-SLM sessions, the configured 'tx-frame-count' value specifies the no. of packets that are sent in a burst at once for On Demand sessions and for every Tx-interval for Scheduled sessions. The timeout will be applicable for the entire burst of frames for On Demand sessions.
- For Two-way ETH-DM sessions, the configured 'tx-frame-count' value specifies total the no. of packets are sent sequentially after every reply message received for on-demand and sent one packet per every Tx-interval for Scheduled (or Periodic) sessions. The timeout is applicable per packet only for On Demand sessions.
- ETH-DM or ETH-SLM if configured over VLAN untagged ports or VPLS untagged endpoints, CoS as per the applied profile would not be applicable and Random CoS (i.e. CoS 8) would be applied instead.
- When Random CoS (i.e. CoS 8) is configured on a test profile and applied on an initiator and responder, a CoS value is randomly chosen between 0-7 before transmission of an DMM or SLM packet. On the responder side, all ETH-DM or ETH-SLM packets for the target MEP are accounted by ignoring the COS. Similar handling is present for DMR or SLR processing as DMM or SLR packet uses the same CoS which was present in the incoming DMM or SLM packet respectively.
- The initiator and responder for a particular ETH-DM or ETH-SLM session should have the same CoS configured on both ends.
- Configurations done under test profiles are persistent after a reload.
- If a profile is updated which is already associated to an active Scheduled Two-way ETH-DM or Scheduled Two-way ETH-SLM session, the current active session(s) will be implicitly

stopped before the profile is updated. The updated profile would be applicable for the next scheduled (or periodic) session(s). However as an exception, if the stop time in the profile associated with an active session is updated to a later time than the current time, the session(s) will not be stopped and the new configured stop time in the profile will be applied immediately.

- DMM/SLM or DMR/SLR packets are not transmitted or received over ports blocked by spanning tree.

Scalability considerations

- A maximum of 128 test profiles can be created on a system.
- A maximum of 32 Two-Way ETH-DM or Two-Way ETH-SLM sessions can be created (by associating maximum of 32 test
- profiles) per source MEP and remote MEP that is RMEP) pair.
- Only one Two-Way ETH-DM and one Two-Way ETH-SLM session can be active per source MEP and remote MEP pair per CoS at any point of time.
- A maximum of 128 Two-Way ETH-DM or Two-Way ETH-SLM scheduled sessions can be activated on a node.
- Only one action profile can be attached to a Source MEP and Target MEP that is RMEP pair. However one action profile can have many event to action(s) associations contained in it.

Configuring Y.1731 Performance Monitoring

To configure the Y.1731 performance monitoring feature on your Extreme device, perform the follow the task.

1. Enter the global configuration mode.

```
device# configure terminal
```

2. Use the **protocol cfm** command to enter the CFM protocol configuration mode

```
device(config)# protocol cfm
```

3. Use the **y1731** command to enter the Y.1731 configuration mode.

```
device(config-cfm)# y1731
```

Creating a test profile

To configure the Y.1731 performance monitoring feature on your Extreme device, perform the following task.

1. Enter the global configuration mode.

```
device# configure terminal
```

2. Use the **protocol cfm** command to enter the CFM protocol configuration mode

```
device(config)# protocol cfm
```

3. Use the **y1731** command to enter the Y.1731 configuration mode.

```
device(config-cfm)# y1731
```

4. Use the **test-profile** command to create a test profile.

```
device(config-cfm-y1731)# test-profile mytest-profile
```

5. Use the **type** command to configure the profile type as ETH-DM or ETH-SLM.

```
device(config-cfm-y1731-mytest-profile)# type delay-management
device(config-cfm-y1731-mytest-profile)# type synthetic-loss-measurement
```

   Enter the **synthetic-loss-measurement** to configure the profile type as ETH-SLM

6. Use the **tx-interval** command to configure the transmission interval.

```
device(config-cfm-y1731-mytest-profile)# tx-interval 10
```

7. Use the **measurement-interval** command to configure the measurement interval.

```
device(config-cfm-y1731-mytest-profile)# measurement-interval 30
```

8. Use the **start** command to configure the start time.

```
device(config-cfm-y1731-mytest-profile)# start 09:00:00
```

9. Use the **stop** command to configure the stop time.

```
device(config-cfm-y1731-mytest-profile)# stop 17:00:00
```

10. Use the **cos** command to configure the class of service (CoS).

```
device(config-cfm-y1731-mytest-profile)# cos 7
```

11. Use the **threshold** command to configure the threshold for the ETH-DM.

```
device(config-cfm-y1731-mytest-profile)# threshold average 4294967295
```

12. Use the **tx-frame-count** command to configure the tx frame count.

```
device(config-cfm-y1731-mytest-profile)# tx-frame-count 50
```

13. Use the **timeout** command to configure the timeout value.

```
device(config-cfm-y1731-mytest-profile)# timeout 3
```

Associating a test profile to an RMEP for scheduled Two-Way ETH-SLM or Two-Way Eth-DM

1. Enter the global configuration mode.

```
device# configure terminal
```

2. Use the **protocol cfm** command to enter the CFM protocol configuration mode.

```
device(config)# protocol cfm
```

3. Use the **domain-name** command to configure a maintenance domain.

```
device(config-cfm)# domain-name m11 id 1 level 4
```

4. Use the **ma-name** command to configure the maintenance association (MA).

```
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
```

5. Use the **mep** command to configure the maintenance end point (MEP).

```
device(config-cfm-md-ma-ma1)# mep 1 down Ethernet 0/2
```

6. Use the **remote-mep** command to configure a remote MEP and associate a test profile.

```
device(config-cfm-md-ma-mep-1)# remote-mep 2 test-profile my_test_profile mode
initiator
```

Configuring an event and actions for an action profile

To configure the Y.1731 performance monitoring feature on your Extreme device, perform the follow the task.

1. Enter the global configuration mode.

```
device# configure terminal
```

2. Use the **protocol cfm** command to enter the CFM protocol configuration mode

```
device(config)# protocol cfm
```

3. Use the **y1731** command to enter the Y.1731 configuration mode.

```
device(config-cfm)# y1731
```

4. Use the **action-profile** command to create an action profile.

```
device(config-cfm-y1731)# action-profile myaction-profile
```

5. Use the **event** command to configure an action profile event and associate actions.

```
device(config-cfm-y1731-myaction-profile)# event avg-threshold actions all
```

Associating an action profile to an RMEP for scheduled Two-Way ETH-SLM or Two-Way Eth-DM

1. Enter the global configuration mode.

```
device# configure terminal
```

2. Use the **protocol cfm** command to enter the CFM protocol configuration mode

```
device(config)# protocol cfm
```

3. Use the **domain-name** command to configure a maintenance domain.

```
device(config-cfm)# domain-name m11 id 1 level 4
```

4. Use the **ma-name** command to configure the maintenance association (MA).

```
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
```

5. Use the **mep** command to configure the maintenance end point (MEP).

```
device(config-cfm-md-ma-ma1)# mep 1 down Ethernet 0/2
```

6. Use the **remote-mep** command to configure a remote MEP and associate an action.

```
device(config-cfm-md-ma-mep-1)# remote-mep 2 action-profile my_action_profile
```

Configuring a scheduled Two-Way ETH-DM or Two-Way ETH-SLM

1. Enter the global configuration mode.

```
device# configure terminal
```

2. Use the **protocol cfm** command to enter the CFM protocol configuration mode.

```
device(config)# protocol cfm
```

3. Use the **domain-name** command to configure a maintenance domain.

```
device(config-cfm)# domain-name md1 id 1 level 4
```

4. Use the **ma-name** command to configure the maintenance association (MA).

```
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
```

5. Use the **mep** command to configure the maintenance end point (MEP).

```
device(config-cfm-md-ma-ma1)# mep 1 down Ethernet 0/2
```

6. Use the **remote-mep** command to configure a scheduled measurement session.

```
device(config-cfm-md-ma-mep-1)# remote-mep 2 test-profile 2dm_default_profile mode
initiator
```

Initiating on-demand Two-Way ETH-DM or Two-Way ETH-SLM

Use the **cfm y1731** command to initiate the on-demand Two-Way ETH-DM or Two-Way ETH-SLM feature.

```
device# cfm y1731 domain md1 ma ma1 src-mep 1 target-mep 2 test-profile
2dm_default_profile
device# cfm y1731 domain md1 ma ma1 src-mep 1 target-mep 2 test-profile
2slm_default_profile
```

Sample VPLS configurations

PE1 sample configuration

The following is a sample configuration on PE 1.

```
interface Loopback 1
no shutdown
ip address 18.1.1.1/32
!

ip route 19.1.1.1/32 1.1.1.19

interface Ethernet 1/2
ip proxy-arp
ip address 1.1.1.18/24
no shutdown
!

interface Ethernet 1/1
switchport
switchport mode trunk
switchport trunk tag native-vlan
logical-interface ethernet 1/1.50
  vlan 50
!
exit
no shutdown
!

bridge-domain 50 P2MP
vc-id 5
peer 19.1.1.1
logical-interface ethernet 1/1.50
no bpdu-drop-enable
pw-profile default
local-switching
!
router mpls
ldp
hello-timeout-target 180
  hello-interval-target 60
  ka-interval 100

mpls-interface ethernet 1/2
  ldp-enable
  ldp-params
   hello-interval 60 hello-timeout 180
```

```
  !
!
```

PE2 sample configuration

The following is a sample configuration on PE 2.

```
interface Loopback 1
no shutdown
ip address 19.1.1.1/32
!

ip route 18.1.1.1/32 1.1.1.18

interface Ethernet 1/1
switchport
switchport mode trunk
switchport trunk tag native-vlan
logical-interface ethernet 1/1.50
  vlan 50
!
exit
!
no shutdown
!
interface Ethernet 1/2
ip proxy-arp
ip address 1.1.1.19/24
no shutdown
!

bridge-domain 50 P2MP
vc-id 5
peer 18.1.1.1
logical-interface ethernet 1/1.50
no bpdu-drop-enable
pw-profile default
local-switching
!
router mpls
ldp
  hello-timeout-target 180
  hello-interval-target 60
  ka-interval 100

mpls-interface ethernet 1/2
  ldp-enable
  ldp-params
   hello-interval 60 hello-timeout 180
  !
!
```

Similar configuration is applicable for VLL with one peer and bridge domain type as P2P.

Sample CFM and Y.1731 configurations

PE1 configuration

The following is a CFM or Y.1731 sample configuration on PE1.

```
protocol cfm
 y1731
  test-profile tp1
   type synthetic-loss-measurement
```

```
    tx-frame-count 1000
    start at 08:05:00
    stop at 08:08:00
   !
  !
  domain-name md1 id 1 level 5
   ma-name ma1 id 1 bridge-domain 50 priority 5
    mep 1 up vlan 50 ethernet 0/1
     remote-mep 2 test-profile tp1 mode initiator
    !
   !
  !
!
```

PE2 configuration

The following is a CFM or Y.1731 sample configuration on PE2.

```
protocol cfm
 y1731
  test-profile tp1
   type synthetic-loss-measurement
   start after 00:00:01
   stop after 00:03:00
  !
 !
 domain-name md3 id 1 level 5
  ma-name ma1 id 1 bridge-domain 50 priority 5
   mep 2 up vlan 50 ethernet 0/1
    remote-mep 1 test-profile tp1 mode responder
   !
  !
 !
!
```

Displaying the Two-Way ETH-DM information

1. Use the **show cfm y1731 delay-measurement** command to display detailed information for all measurement sessions.

   ```
   device# show cfm y1731 delay-measurement
   ```

2. Use the **show cfm y1731 delay-measurement brief** command to display all ETH-DM sessions.

   ```
   device# show cfm y1731 delay-measurement brief
   ```

3. Use the **show cfm y1731 delay-measurement session** command to display detailed information for a particular session. displaying brief ETH-SLM statistics for all sessions.

   ```
   device#: show cfm y1731 delay-measurement session
   ```

4. Use the **show show cfm y1731 delay-measurement statistics** command to display detailed information for all history items for all measurement sessions.

   ```
   device#: show show cfm y1731 delay-measurement statistics
   ```

5. Use the **show cfm y1731 delay-measurement statistics brief** command to display brief history table for each session index.

   ```
   device#: show cfm y1731 delay-measurement statistics brief
   ```

Displaying the Two-Way ETH-SLM Information

1. Use the **show cfm y1731 synthetic-loss-measurement** command to display detailed information for all measurement sessions.

```
device# show cfm y1731 synthetic-loss-measurement
```

2. Use the **show cfm y1731 synthetic-loss-measurement brief** command to display all ETH-SLM sessions in table format.

```
device# show cfm y1731 synthetic-loss-measurement brief
```

3. Use the **show cfm y1731 synthetic-loss-measurement session** command to display detailed information for a particular session. displaying brief ETH-SLM statistics for all sessions.

```
device#: show cfm y1731 synthetic-loss-measurement session 1
```

4. Use the **show cfm y1731 synthetic-loss-measurement statistics brief** command to display brief ETH-SLM statistics for all sessions.

```
device#: show cfm y1731 synthetic-loss-measurement statistics brief
```

5. Use the **show cfm y1731 synthetic-loss-measurement statistics session history** command to display detailed information for a particular history entry for a particular session.

```
device#: show cfm y1731 synthetic-loss-measurement statistics session 1 history 2
```

Displaying Y.1731 profiles

1. Use the **show cfm y1731 test-profile** command to display all profiles including default test profiles and configured test profiles.

```
device# show cfm y1731 test-profile
```

   Use the *profile-name* parameter to display information specific to a particular profile.

2. Use the **show cfm y1731 action-profile** command to display all action profiles.

```
device# show cfm y1731 action-profile
```

   Use the *profile-name* parameter to display information specific to a particular profile.

Clearing Y.1731 statistics

1. Use the **clear cfm y1731 statistics** command to clear statistics for all Y1731 entities.

```
device# clear cfm y1731 statistics
```

2. Use the **clear cfm y1731 statistics delay-mesurement** command to clear all statistics for Two-Way ETH-DM.

```
device# clear cfm y1731 statistics delay-mesurement
```

3. Use the **clear cfm y1731 statistics synthetic-loss-measurement** command to clear all statistics for Two-Way ETH-SLM.

```
device# clear cfm y1731 statistics synthetic-loss-measurement
```

IEEE 802.3ah Ethernet in First Mile

Using Ethernet in the EFM solution, you gain broadcast Internet access, and access to services such as Layer 2 transparent LAN services, voice services over Ethernet access networks, video, and multicast applications. This access is reinforced by security and quality of service

to build a scalable network. The in-band management specified by this standard defines the operations, administration, and maintenance (OAM) mechanism needed for the advanced monitoring and maintenance of Ethernet links in the first mile.

802.3ah protocol in Ethernet

The 802.3ah protocol activities are classified into three layers: transport layer, connectivity layer, and service layer. The transport layer 802.3ah protocol provides single-link OAM capabilities, offering an opportunity to create the operations and OAM sub-layer in the data-link layer. The connectivity layer provides utilities for monitoring and troubleshooting Ethernet links.

The data-link layer protocol targets the last-mile applications. Service providers can use it for demarcation point OAM services. The 802.3ah protocol resolves validation and testing problems. Using the Ethernet demarcation, service providers can additionally manage the remote device without using an IP layer.

The functionality of the 802.3ah protocol is as follows:

- **Discovery**: A mechanism to detect the presence of a sublayer on the remote device. During the process, information about OAM entities, capabilities and configuration are exchanged.
- **Link monitoring**: A process used to detect link faults and to provide information about the number of frame errors and coding symbol errors.

  Note
  Link monitoring functionality is not supported.

- **Remote fault detection**: Provides a mechanism to convey error conditions to its peer via a flag. The failure conditions are defined as follows:
  - **Link Fault**: This fault condition is detected when the receiver loses the signal. This condition is sent one time per second.
  - **Dying Gasp**: This condition is detected when the receiver goes down. The condition is considered as unrecoverable.
  - **Critical Event**: When a critical event occurs, the device is unavailable as a result of malfunction and must be restarted by the user. The critical events are sent immediately and continually.
  - **Remote loopback**: Provides a mechanism to troubleshoot networks and to isolate problem segments in a large network by sending test segments.

Feature support and limitations

Link OAM is a link-level protocol and is supported on physical interfaces.

The following functions are not supported:

- Link monitoring functionality
- Unidirectional support
- SNMP MIB or traps
- UDLD and Link OAM cannot coexist

On SLX-OS devices, Link OAM configuration is allowed on VPLS and VLL endpoints. Support for VPLS and VLL endpoints is available only when Link OAM is configured on the link between CE (passive) and PE (active).

How discovery works

When OAM is present, two connected OAM sub-layers exchange OAM Protocol Data Units (OAMPDU). OAMPDUs are standard-size untagged 802.3 frames that can be sent at a maximum rate of 10 frames per second. A combination of the destination MAC address, the Ethernet type, and subtype distinguishes OAM PDU frames from other frames.

Note
Only Information and loopback Control OAMPDUs are supported.

Network devices are identified with their OAM configuration and capabilities in the discovery phase of the EFM-OAM. Remote loopback configuration and OAM mode (active/passive) capability are supported during this phase.

Note
There is no prerequisite or support for configuration to consider the discovery status as unsatisfied. Any capability received from the peer is considered to be satisfied and will wait for the peer to become stable before marking the Link OAM status as up.

How remote loopback works

Remote loopback allows you to estimate if a network segment can satisfy an SLA and helps you to ensure quality of links during installation and troubleshooting. An OAM entity can put its remote entity into loopback mode using a loopback control OAMPDU. The **remote-loop-back** command allows you to start and stop the remote loopback on peer that is connected to the specified local ethernet interface.

```
device# link-oam remote-loop-back ethernet 1/1 start
device# link-oam remote-loop-back ethernet 1/1 stop
```

Note
As a best practice for loopback mode, you should remove the loopback ports from the active network topology to reduce the impact of protocol flaps. In loopback mode, IP traffic is looped back with the MAC header removed.

For more information about commands, see the *Extreme SLX-OS Command Reference Guide*.

Configuring Link OAM

1. Execute the **link-oam** command to enter the link OAM global configuration mode.

```
device# configure terminal
device(config)# protocol link-oam
device(config-link-oam)#
```

2. (Optional) Execute the **shutdown** command to disable the link OAM protocol. The **no** form of the command enables the protocol.

```
device(config-link-oam)# shutdown
```

   By default, link OAM protocol is enabled when protocol link-oam is configured .

3. Configure the timeout value using the **timeout** command. This value corresponds to the hold time before restarting the discovery process. By default, the timeout value is 5 seconds.

```
device(config-link-oam)# timeout 4
```

4. Configure the PDU rate using the **pdu-rate** command. This value corresponds to the number of OAMPDUs per second. By default, the PDU rate is 1 per second.

```
device(config-link-oam)# pdu-rate 10
```



Note
It is recommended to configure timeout interval at least three times the PDU interval, to avoid link OAM protocol flaps against loss of one or two PDUs for any latency issues in general and during HA Failover.

5. From the Ethernet interface configuration mode, enable the link OAM on the interface using the **link-oam enable** command. By default, link OAM is disabled on the interface.

```
device(config)# interface ethernet 1/1
device(config-int-eth1/1)# link-oam enable passive
```



Note
The mode can be active or passive. The **no** form of the command allows you to remove the current configuration, after which you can reconfigure.

6. Enable the remote loopback functionality in the interface using the **link-oam allow-loopback** command. By default, loopback is disabled on the interface. The **no** form of the command disables the functionality on the interface.

```
device(config-int-eth1/1)#link-oam allow-loopback
```

7. (Optional) Block the interface on receiving the remote failure message using the **link-oam remote-failure** command. By default, on receiving a remote failure message, the device only logs the event through syslog.

```
device(config-int-eth1/1)# link-oam remote-failure link-fault action block-interface
device(config-int-eth1/1)# link-oam remote-failure dying-gasp action block-interface
device(config-int-eth1/1)# link-oam remote-failure critical-event action block-
interface
```



Note
The command configures the block-interface action for each of the three events that the protocol supports.

8. (Optional) Verify the link OAM configuration using the **show link-oam info** command.

```
device# show link-oam info

    Ethernet Link Status OAM Status   Mode     Local Stable    Remote Stable
    1/1      up            up         active     satisfied       satisfied
    1/2      up            up         passive    satisfied       satisfied
```

```
    1/3      up            up         active     satisfied       satisfied
    1/4      up            init       passive    unsatisfied     unsatisfied
    1/5      down          down       passive    unsatisfied     unsatisfied
    1/6      down          down       passive    unsatisfied     unsatisfied
    1/7      down          down       passive    unsatisfied     unsatisfied
```

9. (Optional) View the link OAM statistics using the **show link-oam statistics** command.

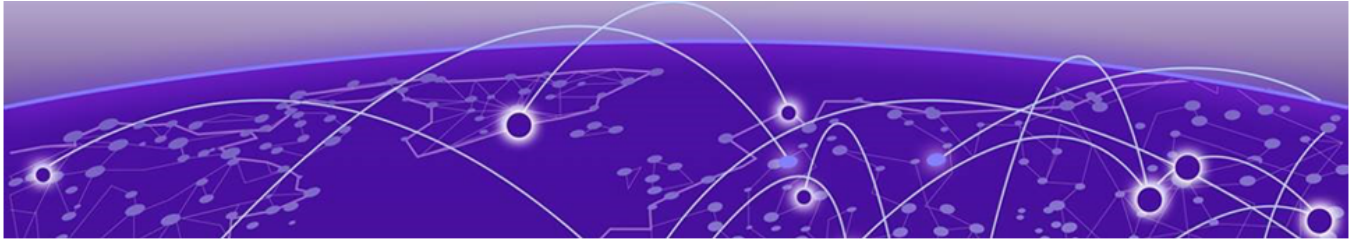
```
device# show link-oam statistics

Ethernet Tx PDUs      Rx PDUs
2/1        93         92
2/2        45         46
```

10. (Optional) From the Exec mode, enable the remote loopback on peer that is connected to local ethernet interface specified, using the **link-oam remote-loop-back** command.

```
device# link-oam remote-loop-back ethernet 1/1 start
device# link-oam remote-loop-back ethernet 1/1 stop
```

11. (Optional) Clear the OAM statistics using the **clear link-oam statistics** command.

```
device# clear link-oam statistics
```



Mirroring

Switched Port Analyzer (SPAN) on page 47
Remote SPAN (RSPAN) on page 47
Encapsulated Remote SPAN (ERSPAN) on page 48
General Considerations when configuring SPAN/RSPAN/ERSPAN on page 48
Flow Based Mirroring on page 50
Configure SPAN Mirroring on page 51
Configuring Flow based SPAN on page 52
Configuring RSPAN Mirroring on page 53
Configuring ERSPAN Mirroring on page 55

Switched Port Analyzer (SPAN)

The analyzer is locally connected to the SPAN destination interface of the SLX device. Unlike a hub, which broadcasts any incoming traffic to all ports, the SLX device forwards traffic accordingly. If you want to snoop on the traffic that passes through a specific port, use port mirroring to copy the packets to a port connected to the analyzer.

You use the **`monitor session`** command to enable a SPAN session. With this command, you can set the packet source, the packet destination, and the packet direction (egress, ingress, or both).

Remote SPAN (RSPAN)

RSPAN enables consolidation of network monitoring at a single location. It works by mirroring target traffic from multiple source ports into a particular VLAN dedicated for monitoring purposes.

The analyzer is connected on the destination switch to the RSPAN VLAN. When this VLAN is trunked to other switches, you can then transport the RSPAN traffic across multiple switches in your network.

You use the **`monitor session`** command to enable a RSPAN session. With this command, you can set the packet source, the packet destination (using the *rspan-vlan* key of this command), and the packet direction (egress, ingress, or both).

Encapsulated Remote SPAN (ERSPAN)

ERSPAN enables monitoring of traffic at multiple source ports and then transmitting this traffic over Layer 3 network to a specific destination port. Multiple source ports can be mirrored to a single destination port. However, you cannot mirror a source port to multiple destination ports.

ERSPAN uses *Generic Routing Encapsulation* (GRE) and thus, is routable across the network.

You use the **`monitor session`** command to enable an ERSPAN session. With this command, you can set the packet source, the packet destination (using the *erspan* key of this command), and the packet direction (egress, ingress, or both).

General Considerations when configuring SPAN/RSPAN/ERSPAN

Keep the following things in mind when configuring SPAN/RSPAN/ERSPAN.

- Do not configure SPAN destination ports to carry normal traffic.
- Configure only physical interfaces and Port Channels as mirror source for Port based mirroring.
- Flow Based Mirroring additionally support VLAN and VE interfaces as source ports.
- The maximum span session configurable per device is 512.
- The standard limitations of forwarding apply to port mirroring when the SPAN source and destination interfaces have different speeds. For example, when traffic is mirrored from a 40G port to a 10G port, the 10G port drops traffic that exceeds the 10G rate.
- In one monitor session configuration, you can have only one SPAN source and only one SPAN destination. However, you can share the same destination port in another session with different source ports. In other words, you can use the same port as a SPAN destination in another SPAN session, which lets you have more SPAN sessions without consuming more SPAN hardware resources.
- ERSPAN Type 3 is the only supported type.
- When configuring flow based monitoring session, mirroring will be enabled when the ACL with mirror action is applied on the source interface in the same direction as in monitor session.
- VLAN configured as RSPAN VLAN should not be used for switching regular traffic.
- When configuring ERSPAN session, make sure that source IP and destination IP belongs to the same VRF.

Considerations for SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720

Keep the following things in mind when configuring SPAN/RSPAN/ERSPAN on SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720 devices.

- The devices support four hardware SPAN sessions.t
  - One unique SPAN destination in the session configuration consumes one hardware SPAN session.
  - Two hardware SPAN sessions are reserved for ACL logging and SPAN sessions created using the legacy **`acl-mirror`** command.

    - Therefore, you can configure two different destinations for port mirroring. If you try to configure mirror sessions with more than two different destination ports, the configuration fails and generates a RASLog message. You have to manually remove the failed configuration.
- CPU-generated frames that do not enter the ingress pipeline of the ASIC cannot be mirrored by an egress SPAN session (an egress SPAN session is enabled on the interface from which the CPU-generated frame egresses). Egress SPAN occurs primarily in the ingress pipeline at the Memory Management Unit (MMU) stage of the ASIC pipeline. For example, a ping that is generated from the device and egresses on a physical Layer 3-routed port does not enter the ingress pipeline. The ping cannot be mirrored by an egress SPAN session.
- The platforms do not support true egress mirroring. If incoming packets are modified and sent to egress ports, some fields, such as VLAN and TTL, in the mirrored captured frames are not identical to the egress frame.
- Because egress SPAN occurs primarily at the MMU stage (which is the last stage of the ingress pipeline of the ASIC), mirrored copy is the same as the packet content seen at this stage. Any VLAN modifications that occurred before this stage are reflected in the mirror copy. However, the original packet can have modifications farther in the egress pipeline and those modifications are not reflected in the mirrored copy.
- Because egress SPAN occurs in the ingress pipeline, the mirroring engine may replicate the egress packets even though the original egress packets could be dropped at later stage. This replication has various causes, such as the source suppression of unknown unicast, broadcast traffic. Source suppression drops unknown traffic before it is transmitted out of the ingress port. However, the replication engine replicates the traffic when the same ingress port is configured as a SPAN source with an egress direction. Therefore, there may not be actual egress frames on the SPAN source interface.
- Flow based egress mirroring is not supported for SPAN, RSPAN, and ERSPAN.
- Flow based ingress mirroring does not support port-channel port as a mirroring source port.
- Flow based ingress mirroring supports VLAN as a mirroring source port, but VLAN range is not supported.

These are the limitations for ERSPAN Type 3 Mirroring.

- For ingress mirroring, copying of VLAN and COS field from original frame to ERSPAN type3 header of mirrored copy is not supported for flow based ERSPAN. It is not supported for Port based ERSPAN and is a hardware limitation.
- For ingress mirroring, if ERSPAN DST IP is reachable through a router port, ERSPAN mirroring will not work.
- Egress mirroring for ERSPAN is not supported due to hardware limitations.

Considerations for SLX 9540 and SLX 9640 devices

Keep the following things in mind when configuring SPAN/RSPAN/ERSPAN on SLX 9540 and SLX 9640 devices.

- SLX 9540 and SLX 9640 do not support RSPAN/ERSPAN. They also do not support the new CLI for configuring flow-based SPAN.
- The devices support fifteen (15) hardware SPAN sessions.
- One unique SPAN destination in the monitor session configuration consumes one hardware SPAN session.
- Twelve sessions are reserved for VxLAN visibility features, snooping applications, and flow-based SPAN sessions.
- Therefore, you can configure three different destinations for port mirroring. If you try to configure mirror sessions with more than three different destination ports, the configuration fails and generates a RASLog message. You have to manually remove the failed configuration.

Considerations for SLX 9740/Extreme 8820 devices

IPV6 ACL based Egress Mirroring is not supported due to hardware limitations across all SPAN types. Only four (4) hardware SPAN sessions are supported. Of the four (4) session, one (1) is reserved for the session created by the legacy **`acl-mirror`** command.

These are the limitations for ERSPAN mirroring.

- In SLX 9740/Extreme 8820 if ingress and egress ERSPAN mirroring is configured to same ERSPAN destination, then the direction field in ERSPAN type 3 header will not have correct values for the mirrored flow.
- ERSPAN ID cannot be set for port based ERSPAN due to hardware limitations.
- For ingress mirroring, copying of VLAN and COS field from original frame to ERSPAN type3 header of mirrored copy is supported for flow based ERSPAN. It is not supported for Port based ERSPAN and is a hardware limitation.

Flow Based Mirroring

Legacy Flow Based Mirroring Configuration

Flow based mirroring enables mirroring of packet flows based on Access Control Lists applied on a port. For Layer 2 ACL Mirroring, see the topic *Layer 2 ACL-based mirroring* in the *Extreme SLX-OS Security Configuration Guide* for this release. Similarly, for Layer 3 ACL Mirroring, see *Layer 3 ACL-based mirroring* in the *Extreme SLX-OS Security Configuration Guide* for this release.

New Flow Based Mirroring Configuration

The new way to configure Flow Based Mirroring is to use the **`monitor session`** command with the keyword *flow-based* when defining the command. Flow based mirroring can be configured for ingress ports of the type *Physical Interface*, *Port Channel*, *VE*, and *VLAN*. The following egress port types can be configured, *Physical Interface*, *Port Channel*, *RSPAN*, and

ERSPAN. The same **monitor session** command is used to configure any combination of Flow Based Mirroring.

Flow Based Mirroring is configured using Access Control Lists (ACLs) and these ACLs are then applied to the specific interface.

Configure SPAN Mirroring

All protocols such as LLDP must be disabled on interfaces that you select to be destination interfaces.

1. Access global configuration mode.

```
SLX # configure terminal
```

2. (If necessary) Disable protocols on the destination interface.

   This example disables LLDP.

   a. Enter interface configuration mode.

```
SLX (config)# interface ethernet 0/2
```

   b. Disable LLDP.

```
SLX (conf-if-eth-0/2)# lldp disable
```

   c. Exit interface configuration mode.

```
SLX (conf-if-eth-0/2)# exit
```

3. Create the port mirroring session and assign a number.

```
SLX (config)# monitor session 22
```

4. Identify the source Ethernet interface port, the destination interface and port (idenitify source interface and destination interface) and the direction of the traffic to monitor. Then create the appropriate mirroring configuration.

```
SLX (config-session-22)# source ethernet 0/1 destination ethernet 0/2 direction tx
```

   This example enables session 22 for monitoring traffic from source Ethernet 0/1 to destination Ethernet 0/2 in the egress direction.

The following example summarizes the commands in this procedure.

```
SLX# configure terminal
SLX (config)# interface ethernet 0/2
SLX (conf-if-eth-0/2)# lldp disable
SLX (conf-if-eth-0/2)# exit
SLX (config)# monitor session 22
SLX (config-session-22)# source ethernet 0/1 destination ethernet 0/2 direction tx
```

The following example shows the configuration of mirroring from a *Port Channel* interface to an *Ethernet* interface. Traffic from both directions is mirrored.

```
SLX# configure terminal
SLX (config)# interface ethernet 0/2
SLX (conf-if-eth-0/2)# lldp disable
SLX (conf-if-eth-0/2)# exit
SLX (config)# monitor session 23
SLX (config-session-23)# source port-channel 1 destination ethernet 0/1 direction both
```

The following example shows the configuration of mirroring from a *Port Channel* to a destination that is a *Port Channel*. Traffic from both directions is mirrored.

```
SLX# configure terminal
SLX (config)# monitor session 24
SLX (config-session-24)# source port-channel 1 destination port-channel 11 direction both
```

Configuring Flow based SPAN

Configuring Flow Based Mirroring requires you to create ACLs that define the rules for the actions that will be performed on the targetted traffic. Multiple ACLs can be created and applied on the target interface. The following limitations apply:

- The following are allowed as source ports, *Physical Ethernet*, *Port Channel*, *VLAN*, or *Virtual Ethernet*.
- The following are allowed as destination ports, *Physical Ethernet* or *Port Channel*.
- You must create your ACLs and apply them to the source ports for mirroring.
- Disable protocols on the destination interfaces.

1. Access global configuration mode.

   ```
   SLX# configure terminal
   ```

2. (If necessary) Disable protocols on the destination interface.

   This example disables LLDP on the destination interface (eth 0/2).

   a. Enter interface configuration mode.

      ```
      SLX (config)# interface ethernet 0/2
      ```

   b. Disable LLDP.

      ```
      SLX (conf-if-eth-0/2)# lldp disable
      ```

   c. Exit interface configuration mode.

      ```
      SLX (conf-if-eth-0/2)# exit
      ```

3. Create an ACL to configure the action to be performed on a traffic type.

   ```
   SLX (config)#ip access-list extended mirror-my-port
   SLX (config-ipacl-ext)#
   ```

4. Add the appropriate rules using the **seq** command. Create as many rules as required. This rule configures mirroring of traffic from 10.10.10.1 in any direction.

   ```
   SLX (config-ipacl-ext)#seq 5 permit ip host 10.10.10.1 any count
   mirror
   ```

5. Exit out of the ACL configuration.

   ```
   SLX (config-ipacl-ext)# exit
   SLX (config)#
   ```

6. Apply the ACL to the source interface.

   ```
   SLX (config)# interface ethernet 0/1
   SLX (config-eth-0/1)# ip access-group mirror-my-port in
   SLX (config-eth-0/1)# ip access-group mirror-my-port out
   ```

7. Enter into the *Monitor Session* mode to configure the mirroring.

   ```
   SLX (config)# monitor session 25
   SLX (config-session-25)# source ethernet 0/1 destination ethernet 0/3 direction both
   flow-based
   ```

This configures the mirroring of the bi-directional traffic from ports 0/1 to 0/3.

This example summarizes the above configuration

```
SLX # configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)#ip access-list extended mirror-my-port
SLX (config-ipacl-ext)#
SLX (config-ipacl-ext)#seq 5 permit ip host 10.10.10.1 any count mirror
SLX (config-ipacl-ext)# exit
SLX (config)# interface ethernet 0/1
SLX (config-eth-0/1)# ip access-group mirror-my-port in
SLX (config-eth-0/1)# ip access-group mirror-my-port out
SLX (config-eth-0/1)# exit
SLX (config)# monitor session 25
SLX (config-session-25)# source ethernet 0/1 destination ethernet 0/3 direction both flow-
based
SLX (config-session-25)# exit
```

This examples show a configuration for Flow Based Mirroring from a *Port Channel* port to an *Ethernet* port.

```
SLX (config)# monitor session 26
SLX (config-session-26)# source port-channel 1 destination ethernet 0/3 direction rx flow-
based
```

This example shows a configuration for Flow Based Mirroring from an *Ethernet* port to a *Port Channel* port.

```
SLX (config)# monitor session 27
SLX (config-session-27)# source ethernet 0/1 destination port-channel 3 direction tx flow-
based
```

This example shows a configuration for Flow Based Mirroring from a *VE* to an *Ethernet* port.

```
SLX (config)# monitor session 28
SLX (config-session-28)# source ve 1 destination ethernet 0/3 direction both flow-
based
```

This example show a configuration for Flow Based Mirroring from a *VLAN* to an *Ethernet* port.

```
SLX (config)# monitor session 29
SLX (config-session-29)# source vlan 100 destination ethernet 0/3 direction tx flow-
based
```

Configuring RSPAN Mirroring

Do the following to configure RSPAN Mirroring where the source port is a *Physical Ethernet* port and the destination ports are a *RSPAN VLAN* and another *Physical Ethernet* port.

1. Access global configuration mode.

   ```
   SLX# configure terminal
   ```

2. (If necessary) Disable protocols on the destination interface.

   This example disables LLDP.

   a. Enter interface configuration mode.

      ```
      SLX (config)# interface ethernet 0/2
      ```

b. Disable LLDP.

```
SLX (conf-if-eth-0/2)# lldp disable
```

c. Exit interface configuration mode.

```
SLX (conf-if-eth-0/2)# exit
```

3. Create the port mirroring session and assign a number.

```
SLX (config)# monitor session 28
SLX (config-session-28)#
```

4. Identify the source Ethernet interface port, the destination RSPAN VLAN, the interface and port (for the ethernet port through which the RSPAN VLAN is reachable), and the direction of the traffic to monitor. Then create the appropriate mirroring configuration.

```
SLX (config-session-28)# source ethernet 0/1 destination rspan-vlan 120 ethernet
0/3         direction rx
SLX (config-session-28)#
```

The ingress traffic on ethernet port 0/1 is now mirrored to the destination RSPAN VLAN through the configured ethernet port.

This example summarizes the above configuration

```
SLX# configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)# monitor session 28
SLX (config-session-28)# source ethernet 0/1 destination rspan-vlan 120 ethernet 0/3
direction rx
```

This example shows the configuration of RSPAN mirroring from a source ethernet port to a destination RSPAN VLAN on a port channel.

```
SLX (config)# monitor session 30
SLX (config-session-30)# source ethernet 0/1 destination rspan-vlan 120 port-channel 2
direction tx
```

Configuring Flow based RSPAN

The following example shows the configuration of Flow Based Mirroring.

The following example shows the configuration of Flow Based Mirroring of an *ethernet* port to a RSPAN VLAN.

```
SLX # configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)#ip access-list extended mirror-my-port
SLX (config-ipacl-std)#
SLX (config-ipacl-std)#seq 5 permit ip host 10.10.10.1 any count mirror
SLX (config-ipacl-std)# exit
SLX (config)# interface ethernet 0/1
SLX (config-eth-0/1)# ip access-group mirror-my-port in
SLX (config-eth-0/1)# ip access-group mirror-my-port out
SLX (config-eth-0/1)# exit
```

```
SLX (config)# monitor session 25
SLX (config-session-25)# source ethernet 0/1 destination rspan-vlan 120 ethernet 0/3
direction both flow-based
SLX (config-session-25)# exit
```

The following example shows the configuration of Flow Based Mirroring of a *VLAN* to a RSPAN VLAN accessible on a port channel.

```
SLX # configure terminal
SLX (config)#mac access-list extended mirror-my-port
SLX (config-ipacl-std)#
SLX (config-ipacl-std)#seq 5 permit ip host 10.10.10.1 any count mirror
SLX (config-ipacl-std)# exit
SLX (config)# vlan 100
SLX (config-vlan-100)# ip mac access-group mirror-my-port in
SLX (config-vlan-100)# ip mac access-group mirror-my-port out
SLX (config-vlan-100)# exit
SLX (config)# monitor session 31
SLX (config-session-31)# source vlan 100 destination rspan-vlan 120 port-channel 2
direction both flow-based
SLX (config-session-31)# exit
```

Configuring ERSPAN Mirroring

Do the following to configure ERSPAN Mirroring where the source port is a *Physical Ethernet* port and the destination ports are a *RSPAN VLAN* and another *Physical Ethernet* port.

1. Access global configuration mode.

   ```
   SLX# configure terminal
   ```

2. (If necessary) Disable protocols on the destination interface.

   This example disables LLDP.

   a. Enter interface configuration mode.

      ```
      SLX (config)# interface ethernet 0/2
      ```

   b. Disable LLDP.

      ```
      SLX (conf-if-eth-0/2)# lldp disable
      ```

   c. Exit interface configuration mode.

      ```
      SLX (conf-if-eth-0/2)# exit
      ```

3. Create the port mirroring session and assign a number.

   ```
   SLX (config)# monitor session 32
   SLX (config-session-32)#
   ```

4. Identify the source Ethernet interface port, the destination port, and the direction of the traffic to monitor. Then create the appropriate mirroring configuration. The GRE tunnel is automatically created between the source and the destination ports.

   ```
   SLX (config-session-32)# source ethernet 0/1 destination erspan 1 source-ip
                          10.10.10.1 destination-ip 10.20.20.1 vrf vrf-for-erspan
   direction both
   SLX (config-session-28)#
   ```

The ingress traffic on ethernet port 0/1 will now be mirrored to the IP 10.20.20.1 over GRE tunnel.

This example summarizes the above configuration

```
SLX# configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)# monitor session 32
SLX (config-session-32)# source ethernet 0/1 destination erspan 1 source-ip 10.10.10.1
        destination-ip 10.20.20.1 vrf vrf-for-erspan direction both
```

This example shows the configuration of ERSPAN mirroring from a source port channel port to a destination IP over GRE.

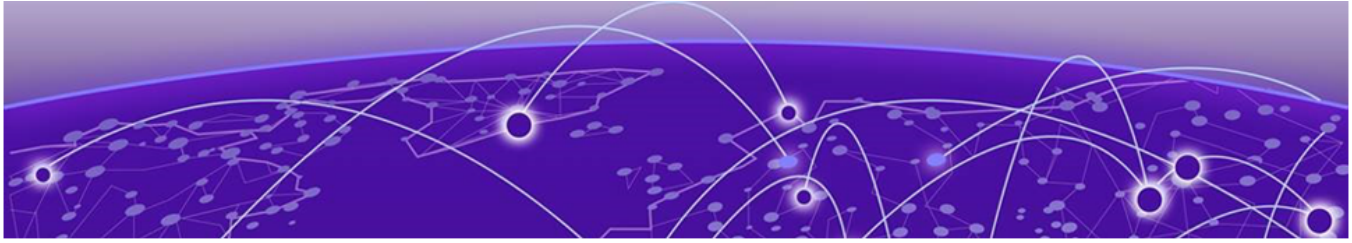
```
SLX (config)# monitor session 33
SLX (config-session-33)# source port-channel 1 destination erspan 1 source-ip 10.10.10.1
        destination-ip 10.20.20.1 vrf vrf-for-erspan direction both
```

This example shows the configuration of ERSPAN mirroring from a VE (ve 1) to an specific destination IP(10.20.20.1). This traffic is directed over IP GRE tunnel with a source IP (10.10.10.1).

```
SLX (config)# monitor session 34
SLX (config-session-34)# source ve 1 destination erspan 1 source-ip 10.10.10.1
destination-ip 10.20.20.1
        direction rx vrf vrf-for-erspan flow-based
SLX (config-session-34)# exit
```

This example shows the configuration of ERSPAN mirroring from a VLAN (vlan 100) to an specific destination IP(10.20.20.1). This traffic is directed over IP GRE tunnel with a source IP (10.10.10.1).

```
SLX (config)# monitor session 34
SLX (config-session-34)# source vlan 100 destination erspan 1 source-ip 10.10.10.1
destination-ip 10.20.20.1
        direction rx vrf vrf-for-erspan flow-based
SLX (config-session-34)# exit
```



Network-Elements Telemetry

Network-elements telemetry overview on page 57
Telemetry profiles on page 57
External-collector streaming on page 61
gRPC-server streaming on page 63

Network-elements telemetry overview

Telemetry *profiles* are basic elements of the various SLX-OS telemetry implementations. Each profile is designed to monitor a specific grouping of data, for example, queue or interface statistics. For profile descriptions and implementation, refer to Telemetry profiles on page 57.

Telemetry data collected on the network elements is transmitted using two approaches:

- External-collector streaming on page 61
- gRPC-server streaming on page 63

You can stream telemetry concurrently to no more than six collectors and gRPC clients.

Telemetry profiles

Note
For MPLS telemetry-profiles (SLX 9540 and SLX 9640 only), refer to the "MPLS traffic statistics data streaming" section of the *Extreme SLX-OS MPLS Configuration Guide*.

Profiles contain the following elements:

- Attributes (usually counters), which you can selectively remove from the profile
- An interval value (how often data are sent), which you can modify
- (Most profiles) The interfaces that you want the profile to monitor

The following telemetry profile types and profiles are supported:

interface

Of the interface profile-type, the only profile supported is **`default_interface_statistics`**. This profile tracks data related to the physical interface. You need to specify monitored interfaces and can modify the default streaming interval.

The fields supported by default for this profile are as follows:

- In/Out packets
- In/Out unicast packets
- In/Out broadcast packets
- In/Out multicast packets
- In/Out packets per second
- In/Out octets
- In/Out errors
- In/Out CRC errors
- In/Out discards

system-utilization

Of the system-utilization profile-type, the only profile supported is **`default_system_utilization_statistics`**. This profile tracks system-related data. You can modify the default streaming interval.

The fields supported by default for this profile are as follows:

- Total system memory
- Total used memory
- Total free memory
- Cached memory
- Buffers
- Total swap memory
- Total free swap memory
- Total used swap memory
- User process
- System process
- Niced process
- In/Out wait
- Hw interrupt
- Sw interrupt
- Idle State
- Steal time
- Uptime

Queue profiles



Note
Queue profiles are supported only on the SLX 9540 and SLX 9640 devices.

Of the queue profile-type, the only profile supported is default_queue_statistics. This profile tracks data related to the queue. You need to specify monitored interfaces and can modify the default streaming interval.

Of the enhanced-queue-discard-pkts profile-type, the only profile supported is enhanced-queue-discard-pkts. This profile tracks data related to discarded packets. You need to specify monitored interfaces and can modify the default streaming interval.

Of the enhanced-queue-max-queue-depth profile-type, the only profile supported is default_enhanced_queue_max_queue_depth_statistics. This profile tracks data related to maximum queue depth. You need to specify monitored interfaces and can modify the default streaming interval.

The following table summarizes profile support for queue data.

Table 8: Profile support for queue data

Profile	Description
default_enhanced_queue_discard_pkts_statistics	Captures summary of 32 queues having the most number of packets discarded, in descending order of packet discards observed. Indexed by interface (slot/port). Data stream contains: • Slot-id • Device-id (~Ifindex) • Queue-id • Discard Packet Counts
default_enhanced_queue_max_queue_depth_statistics	Captures summary of 32 queues reaching maximum max-queue-size, in descending order. Data stream contains: • Slot-id • Device-id (~Ifindex) • Queue-id • Max-Queue-Depth
default_queue_statistics	Captures all queue statistics per specified interface. Data stream contains: • Slot-id • Device-id (~Ifindex) • Queue-id • EnQ Pkt Count • EnQ Byte Count • Discard Pkt Count • Discard Byte Count • Current Queue Size • Max Queue Depth Slze

Configuring telemetry profiles

1. In privileged EXEC mode, enter **configure terminal**.

```
device# configure terminal
```

2. Enter the **telemetry profile** command to configure the profile.

```
device(config)# telemetry profile interface default_interface_statistics
```

3. (For interface profile-type) Enter the **interface** command, specifying the interface range to monitor.

```
device(config-interface-default_interface_statistics)# interface 0/1-2,0/7
```

4. (For other profiles that require specifying interfaces) Enter the **interface-range** command, specifying the interface range to monitor.

```
device(config-queue-default_queue_statistics)# interface-range 0/1-2,0/7
```

5. To modify the default interval, enter the **interval** command.

```
device(config-interface-default_interface_statistics)# interval 30
```

6. To remove a default attribute, enter the **no add** command.

```
device(config-system-utilization-default_system_utilization_statistics)# no add buffers
```

7. To restore a default attribute that was previously removed, enter the **add** command.

```
device(config-system-utilization-default_system_utilization_statistics)# add buffers
```

8. To restore all default attributes, enter the **telemetry reset profile** command.

```
device(config-system-utilization-default_system_utilization_statistics)# do telemetry
reset profile interface-profile
```

9. To specify a VRF other than the default mgmt-vrf, enter the **use-vrf** command.

```
device(config-interface-default_interface_statistics)# use-vrf blue_vrf
```

10. To exit configuration mode—saving the configuration—enter **exit**.

```
device(config-interface-default_interface_statistics)# exit
```

The following example specifies the monitored interfaces and changes the default interval.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interval 30
device(config-interface-default_interface_statistics)# interface 0/1-2,0/7
device(config-interface-default_interface_statistics)# exit
```

Configuring queue telemetry profiles

1. In privileged EXEC mode, enter **configure terminal**.

```
device# configure terminal
```

2. Enter the **telemetry profile** command to configure the profile.

```
device(config)# telemetry profile enhanced-queue-discard-pkts
default_enhanced_queue_discard_pkts_statistics
```

3. Configure the interface range for the profile.

```
device(enhanced-queue-discard-pkts-default_enhanced_queue_discard_pkts_statistics)#
interface-range 1/2-3,2/1-3
```

4. (If needed) Modify the delay interval for the profile.

```
device(enhanced-queue-discard-pkts-default_enhanced_queue_discard_pkts_statistics)#
interval 2005
```

5. Confirm the profile configuration with the **show running-config telemetry profile** command.

```
device(enhanced-queue-discard-pkts-default_enhanced_queue_discard_pkts_statistics)# do
show running-config telemetry profile enhanced-queue-max-queue-depth
telemetry profile enhanced-queue-discard-pkts
default_enhanced_queue_discard_pkts_statistics
interval 2005
interface-range 1/2-3,2/1-3
add discard pkts
```

External-collector streaming

For each target collector device, you configure a local **telemetry collector** object that specifies the following parameters:

- One or more telemetry profiles
- IPv4 address/port of the collector device
- Encoding format (Google protocol buffers (GPB) or JavaScript object notation (JSON))
- (Optional) VRF
- Activation

The following diagram depicts the many-to-many relationships between profiles and collectors:

- You can specify multiple profiles in a collector.
- You can specify a profile in multiple collectors.

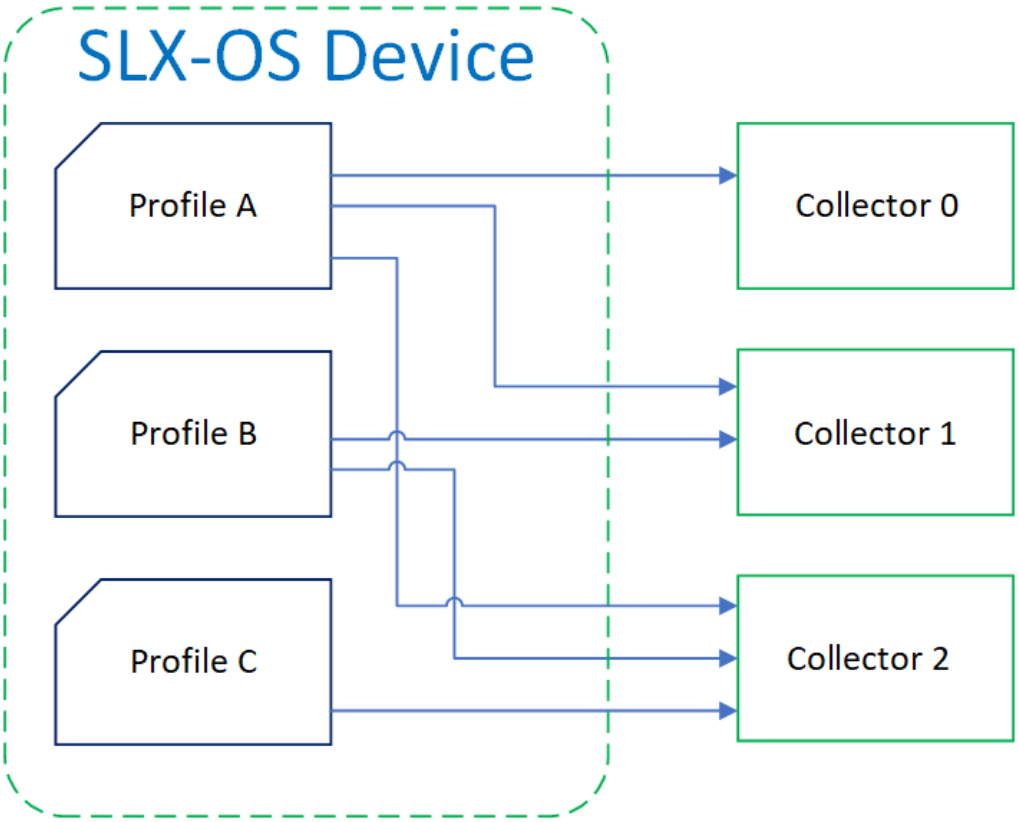


Figure 9: Profile/collector relationships in external-collector streaming

Note
The preceding diagram does not depict local **`telemetry collector`** objects.

Configuring telemetry collectors

1. In privileged EXEC mode, enter **`configure terminal`**.

```
device# configure terminal
```

2. Enter the **`telemetry collector`** command, specifying a collector name.

```
device(config)# telemetry collector collector_1
```

3. Enter the **`ip port`** command, specifying the IPv4 address and port of the collector.

```
device(config-collector-collector_1#) ip 10.168.112.10 port 1
```

4. Enter the **`profile`** command to add one or more telemetry profiles.

```
device(config-collector-collector_1)# profile system-profile
default_system_utilization_statistics
device(config-collector-collector_1)# profile interface-profile
default_interface_statistics
```

5. To specify a VRF context other than mgmt-vrf, enter the **`use-vrf`** command.
6. Enter the **`encoding`** command to specify the encoding format.

```
device(config-collector-collector_1)# encoding ?
Possible completions:
```

```
  gpb    Google protobuf encoding
  json   JSON encoding
device(config-collector-collector_1)# encoding json
```

7. Enter the **activate** command to activate the collector.

```
device(config-collector-collector_1)# activate
```

8. To confirm the configuration, enter the **show running-configuration telemetry collector** command.

```
device(config-collector-collector_1)# do show running-configuration telemetry collector
telemetry collector <collector-profile-1>
  ip <ipv4address1> port <portNum>
  profile system-utilization default_system_utilization_statistics
  profile interface default_interface_statistics
  use-vrf mgmt-vrf
  encoding json
  activate
```

9. To display the status of a telemetry collector, enter the **show telemetry collector** command.

```
device(config-collector-collector_1)# do show telemetry collector collector_1
Telemetry data is streamed to collector_1 on 10.128.116.10 and port 1, with transport
as tcp.

Profiles Streamed                     Interval   Uptime      Last Streamed
------------------                    ---------  ----------  ---------------
default_interface_statistics          120 sec    05/10:23    2017-01-15: :05:07:33
default_system_utilization_statistics 300 sec    05/10:23    2017-01-15: :05:07:33
!
```

10. To display the status of active telemetry collector sessions, enter the **show telemetry collector summary** command.

```
device# show telemetry collector summary
Activated Collectors:
--------------------
Name              IP Address:Port       Streaming/Connection Status
-------------     --------------------  ---------------------------
 coll1            10.24.65.182:9000     connection_failed
```

The following example configures and activates a telemetry collector.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-collector-collector_1)# profile system-profile
default_system_utilization_statistics
device(config-collector-collector_1)# profile interface-profile
default_interface_statistics
device(config-collector-collector_1)# ip 10.168.112.10 port 1
device(config-collector-collector_1)# encoding json
device(config-collector-collector_1)# activate
```

gRPC-server streaming

The telemetry profiles currently configured with interfaces determine the monitored attributes and the streaming intervals. For details, refer to Telemetry profiles on page 57. Client RPCs must be crafted to request streaming per telemetry profile.

The **telemetry server** command offers an option to specify a VRF other than the default mgmt-vrf.

From telemetry-server configuration mode, you can modify the following default settings:

- Port: 50051
- Transport protocol: TCP, which can be modified to SSL.

From telemetry-server configuration mode, you also activate and deactivate the gRPC server.

The following diagram illustrates the gRPC-server telemetry implementation:

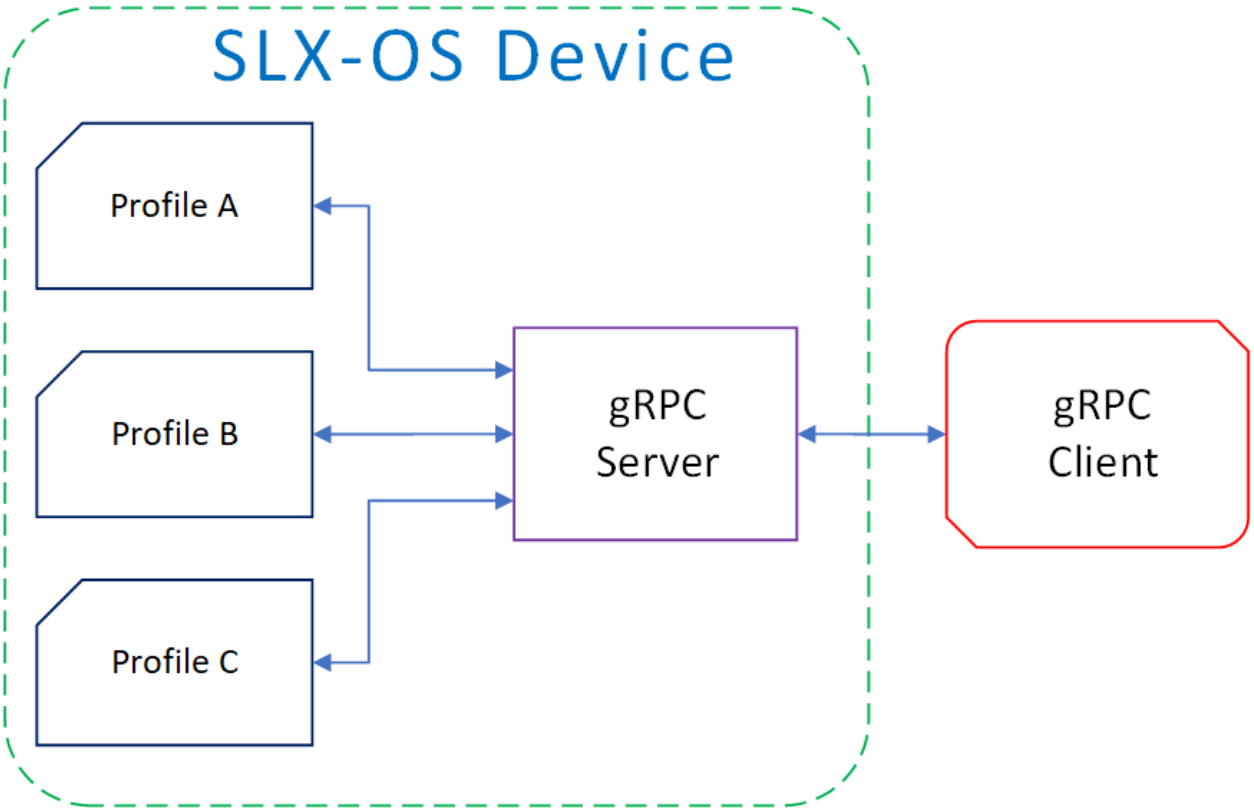


Figure 10: gRPC-server streaming

Configuring the gRPC telemetry server

1. In privileged EXEC mode, enter **`configure terminal`**.

```
device# configure terminal
```

2. Enter **`telemetry server`**, with the option of specifying a VRF other than the default mgmt-vrf.
   - (Default) mgmt-vrf

```
device(config)# telemetry server
```

   - Other VRF

```
device(config)# telemetry server use-vrf blue_vrf
```

3. To specify a port other than the default 50051, enter the **`port`** command.

```
device(config-server-mgmt-vrf)# port 50000
```

4. Enter **activate**.

```
device(config-server-mgmt-vrf)# activate
```

5. Verify the telemetry server status with the **do show telemetry server status** command. The active sessions displayed are initiated by gRPC clients with associated telemetry profiles.

```
device(config-server-mgmt-vrf)# do show telemetry server status

Telemetry Server running on port 50051, with VRF mgmt-vrf and transport as tcp.

Active Sessions:
----------------
Client            Profiles Streamed                      Interval   Uptime      Last
Streamed
------            -----------------                      ---------  ----------
---------------
ClientIP1/Host1   default_interface_statistics           120 sec    05/10:23
2017-01-15: :05:07:33
                  default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33

ClientIP2/Host2   default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33
```

6. Verify the telemetry server configuration with the **do show running-configuration telemetry server** command.

```
device(config-server-mgmt-vrf)# do show running-configuration telemetry server

telemetry server
  transport tcp
  port 50051
  activate
!
```

The following is a complete telemetry server configuration example.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)# activate
device(config-server-mgmt-vrf)# do show telemetry server status

Telemetry Server running on port 50051, with VRF mgmt-vrf and transport as tcp.

Active Sessions:
----------------
Client            Profiles Streamed                      Interval   Uptime      Last
Streamed
------            -----------------                      ---------  ----------
---------------
ClientIP1/Host1   default_interface_statistics           120 sec    05/10:23
2017-01-15: :05:07:33
                  default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33

ClientIP2/Host2   default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33
device(config-server-mgmt-vrf)# do how running-configuration telemetry server

telemetry server
  transport tcp
  port 50051
  activate
```

```
!
```

Configuring SSL on the gRPC telemetry server

1. In privileged EXEC mode, enter **configure terminal**.

```
device# configure terminal
```

2. Enter **telemetry server**, with the option of specifying a VRF other than the default mgmt-vrf.
   - (Default) mgmt-vrf
     ```
     device(config)# telemetry server
     ```
   - Other VRF
     ```
     device(config)# telemetry server use-vrf blue_vrf
     ```
3. Enter the **activate** command.

```
device(config-server-mgmt-vrf)# activate
```

4. Enter **do telemetry client-cert generate** to generate SSL certificates for the server and client.

```
device(config-server-mgmt-vrf)# do telemetry client-cert generate
```

5. Verify the certificate is active with the **do show telemetry client-cert** command.

   This output displays the SSL public CA certificate that is used for secure connections on the client side for establishing SSL connections, such as streaming with recipients for gRPC clients or destinations.

```
device(config-server-mgmt-vrf)# do show telemetry client-cert

-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoMB0Jyb2NhZGUxEjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xNzAzMjExNzQ1NDNa
Fw0xODAzMjExNzQ1NDNaMDMxCzAJBgNVBAYTAkNBMRAwDgYDVQQKDAdCcm9jYWRl
MRIwEAYDVQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC+YG/CkiNm/BO+u1mYLKP8cpz/0O9CE+fusO0spXxjKfjPAvK7kiogxABm
bg9MQeWl4SbFa5x3q5uyZJxApJ+tAnnWZa+cbj5pmNsQFfIbFOwSAmFyhh/NIp7Y
/wApskKjnVsMFkarqX8W2xKxZreapZFMa9DGpOeh8Jo2yvcTAimFfSJ4nyKlCr1C
DuuaTSvAttC8Z9mEqD9TOaSYwQI0pnfVO+ySgY8ndqDXYdRvl+bV1taghlKOgxMY
J78lyZxYf6CIn22BAaz/f9a5ffS13Hh5Cmurj2dUmmqDE49p2KEVtXQ3D6nuopli
V49ok+z93/40Uq4OVJZJk5Kx8ZuxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAI1d
1VkMH9i3SorPIHpbVqbeDe7LPdaFmrT0COr3AFUECw3gBj1Zy82Kp8XkIJJdVCu8
MNm3wTARqeNBY2c3luw6QeA6l4qRIVM4FqNj6rvtqtNZQ9EEKRRwAm0GSVp+uSvu
E88XSXO+r6N+SXQemRIyhNQ7LJq+cDEaP5WfNtKg+zj085Xd0qiB94BKFt5Q+xAa
B7lwuUvT7Yt92aUVXIaZ6aY5oMv4t7+lPBBKjg8cNeywDa9h3yVZYIzSggghu0qu
GZO57qUh5agxqKiEVf9Ya325u5gj73UJsKOSsyVA1HB8RsPEEdz8j8FBAqMNSTQj
8UDtUGpYiYlzyiBUELc=
-----END CERTIFICATE-----
```

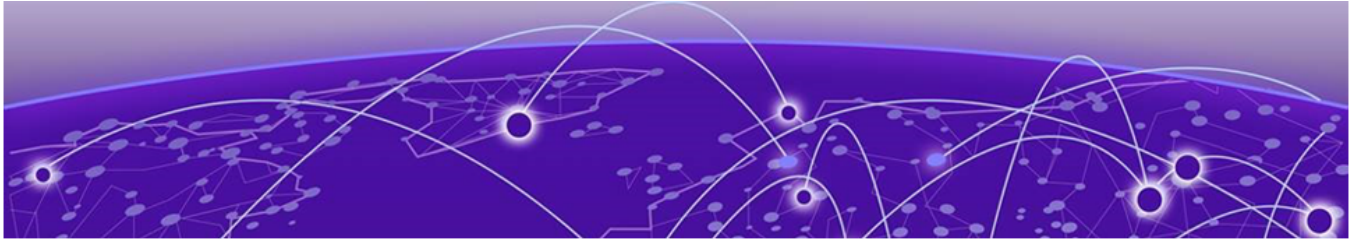
6. Enter **transport ssl**.

```
device(config-server-mgmt-vrf)# transport ssl
```

The following example is a complete SSL configuration example.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)# activate
device(config-server-mgmt-vrf)# do show telemetry server status
```

```
Telemetry Server running on IP 10.128.116.10 and port 1, with transport as tcp.

Active Sessions:
----------------
Client            Profiles Streamed                      Interval   Uptime      Last
Streamed
------            -----------------                      ---------  ----------
---------------
ClientIP1/Host1   default_interface_statistics           120 sec    05/10:23
2017-01-15: :05:07:33
                  default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33

ClientIP2/Host2   default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33

device(config-server-mgmt-vrf)# do telemetry client-cert generate
device(config-server-mgmt-vrf)# do show telemetry client-cert

-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoMB0Jyb2NhZGUxEjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xNzAzMjExNzQ1NDNa
Fw0xODAzMjExNzQ1NDNaMDMxCzAJBgNVBAYTAkNBMRAwDgYDVQQKDAdCcm9jYWRl
MRIwEAYDVQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC+YG/CkiNm/BO+u1mYLKP8cpz/0O9CE+fusO0spXxjKfjPAvK7kiogxABm
bg9MQeWl4SbFa5x3q5uyZJxApJ+tAnnWZa+cbj5pmNsQFfIbFOwSAmFyhh/NIp7Y
/wApskKjnVsMFkarqX8W2xKxZreapZFMa9DGpOeh8Jo2yvcTAimFfSJ4nyKlCr1C
DuuaTSvAttC8Z9mEqD9TOaSYwQI0pnfVO+ySgY8ndqDXYdRvl+bV1taghlKOgxMY
J78lyZxYf6CIn22BAaz/f9a5ffS13Hh5Cmurj2dUmmqDE49p2KEVtXQ3D6nuopli
V49ok+z93/40Uq4OVJZJk5Kx8ZuxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAI1d
1VkMH9i3SorPIHpbVqbeDe7LPdaFmrT0COr3AFUECw3gBj1Zy82Kp8XkIJJdVCu8
MNm3wTARqeNBY2c3luw6QeA6l4qRIVM4FqNj6rvtqtNZQ9EEKRRwAm0GSVp+uSvu
E88XSXO+r6N+SXQemRIyhNQ7LJq+cDEaP5WfNtKg+zj085Xd0qiB94BKFt5Q+xAa
B7lwuUvT7Yt92aUVXIaZ6aY5oMv4t7+lPBBKjg8cNeywDa9h3yVZYIzSggghu0qu
GZO57qUh5agxqKiEVf9Ya325u5gj73UJsKOSsyVA1HB8RsPEEdz8j8FBAqMNSTQj
8UDtUGpYiYlzyiBUELc=
-----END CERTIFICATE-----
device(config-server-mgmt-vrf)# transport ssl
device(config-server-mgmt-vrf)# do show telemetry server status

Telemetry Server running on IP 10.128.116.10 and port 1, with transport as ssl.

Active Sessions:
----------------
Client            Profiles Streamed                      Interval   Uptime      Last
Streamed
------            -----------------                      ---------  ----------
---------------
ClientIP1/Host1   default_interface_statistics           120 sec    05/10:23
2017-01-15: :05:07:33
                  default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33

ClientIP2/Host2   default_system_utilization_statistics  300 sec    05/10:23
2017-01-15: :05:07:33
```



Hardware Monitoring

Hardware monitoring overview on page 68
Cyclic redundancy check (CRC) on page 97
High and Low watermarks for port utilization on page 98

Hardware monitoring overview

Policies can be created with default options or custom options for non-default thresholds. When the policies are applied, you can toggle between default settings and saved custom configuration settings and apply actions and thresholds separately. For example, you can choose to use default threshold settings together with a customized subset of available actions, or you can modify some of the threshold settings and use the default action settings. You can also pause monitoring and actions.

System Resource Monitoring (SRM)

This helps you to take adequate actions before the system reaching fatal state. This automated information gathering helps to identify those processes which are involved in high memory usage and assist in debugging memory leakage. Based on this information, you can amend configurations to avoid pushing the resource usage over the limit. SupportSave data is also collected so that the root cause of the issue can be analyzed offline and fixed.

With the per-process memory monitoring service enabled, if the high memory usage threshold is crossed for any of the processes, an **alarm** message is generated. If memory usage still goes up to another threshold, a **critical** message is generated. Based on the information available, the resolution has to be worked out manually.

If the system memory monitoring service is enabled, SRM generates raslog to notify that the system memory usage crossed the set threshold. If the CPU utilization monitoring service is enabled, SRM generate raslog to notify that the CPU usage exceeded threshold of 90%.

This functionality is provided by the **`resource-monitor`** command.

Configuring system resource monitoring

1. Enter global configuration mode.

```
device# configure terminal
```

2. Issue the **resource-monitor cpu enable** command to enable the CPU utilization monitoring service.

```
device(config)# resource-monitor cpu enable
```

3. Issue the **resource-monitor memory** command to enable the system memory monitoring and generate raslog when the memory usage exceeds threshold value.
4. Issue the **resource-monitor process memory** command to enable the per-process memory monitoring and generate alarm or raslog when the usage exceeds alarms threshold or critical threshold respectively.
5. (Optional) Issue the how running-configuration command to view the resource monitoring running configuration.

CPU, memory, and buffer monitoring

When configuring CPU monitoring, specify a value in the 1-100 range. When the CPU usage exceeds the limit, a threshold monitor alert is triggered. The default CPU limit is 75 percent. With respect to memory, the limit specifies a usage limit as a percentage of available resources.

When used to configure memory or CPU threshold monitoring, the limit value must be greater than the low limit and smaller than the high limit.

Monitoring involves automatic data gathering for low memory and buffer conditions and high CPU conditions. Threshold monitoring tracks the buffer thresholds for each BM buffer queues and the buffer usage on periodic interval and undertake the defined actions whenever the threshold exceeds.

Memory status data collection is invoked by SRMd and is collected every hour. Data collection is triggered upon reaching the limit . The data is available at */var/log/mstatdir* and includes historic data.

The histogram feature includes the functionality to collect detailed CPU, memory and buffer utilization by system tasks. This is used to troubleshoot resource allocation and utilization problems. It also includes functionality to monitor line module memory errors. Error messages are logged via Syslog and SNMP traps.

As part of CPU threshold monitoring, some packets that are received by CPU are captured and stored in non-volatile RAM, when CPU hits an abnormal level. This serves and historic reference data for support engineers to troubleshoot network outage.

The alert provided is a RASLog message, with the following options configurable under the raslog option of the **threshold-monitor cpu** , **threshold-monitor buffer** or the **threshold-monitor memory** commands:

Limit specifies the baseline memory usage limit as a percentage of available resources. When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by limit, a RASLog INFO message is sent. Valid values range from 0 through 80 percent.

High-limit Specifies an upper limit for memory usage as a percentage of available memory. This value must be greater than the value set by limit. When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Valid values range from range from 0 through 80 percent.

The **show process cpu top** command collects those CPU usages which crosses the threshold value. This data is logged into a text file so that it can be read offline.

Low-limit specifies a lower limit for memory usage as percentage of available memory. This value must be smaller than the value set by limit.

The low memory condition is not prevented. When memory usage exceeds or falls below this limit, the **threshold-monitor** command reports in RASLog and a RASLog information message is sent.

Poll specifies the polling interval in seconds. Valid values range from 0 through 3600.

Retry specifies the number of polling retries before desired action is taken. Valid values range from 1 through 100.



Note
For CPU and memory thresholds, the low limit must be the lowest value and the high limit must be the highest value.

The following actions are configurable when the set threshold is violated:

- raslog - RASLOG will be sent
- none- No action will be taken
- loginfo- Diagnostic data collection along with RASLOG



Note
The loginfo action collects the '*show process cpu top*' and *iostat* information into a file.

The table below lists the factory defaults for CPU, memory, and buffer thresholds.

Table 9: Default values for CPU, memory, and buffer threshold monitoring

Operand	Memory	CPU	Buffer
low-limit	40%	N/A	N/A
limit	60%	75%	70%
high-limit	70%	N/A	N/A
poll	120 seconds	120 seconds	120 seconds
retry	3	3	N/A

Configuring hardware monitoring for CPU, memory, and buffer usage

When monitoring is configured, thresholds can be set. When the thresholds are exceeded, actions such as messages can be sent. Logs are saved for periods of time to enable viewing of threshold status.

Note
Support for the custom policy operand is not provided for CPU and memory threshold monitoring.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To set the memory threshold between 40 and 60 and cause no message to be sent when thresholds are exceeded, enter the **threshold-monitor memory** command as follows.

```
device(config)# threshold-monitor memory actions none high-limit 60 low-limit 40
```

3. To adjust cpu usage polling and retry attempts and cause a RASLog message to be sent and collect more diagnostic information when thresholds are exceeded, enter the **threshold-monitor cpu** command as follows.

```
device(config)# threshold-monitor cpu actions loginfo limit 65 poll 60 retry 10
```

4. To set the buffer utilization threshold at 75% and polling interval as 130 seconds, enter the **threshold-monitor buffer** command as follows.

```
device(config)# threshold-monitor Buffer limit 75 poll 130 actions loginfo
```

Viewing threshold status

To view the status of currently configured thresholds, enter the **show running-config threshold-monitor** command, as follows:

```
device(config)# show running-config threshold-monitor
```

Note
Default values are not displayed under the **show running-config threshold-monitor** command. Only custom values are displayed when a user applies a policy.

Optical monitoring

Once an optic is detected by the software, it reads the erasable programmable read only memory (EPROM) to determine if it is Extreme certified. The data is read periodically to monitor the health. If it is not able to access the EPROM of any optic, that particular optic is put into failed state and the port link will not come up. Optics which are not certified by Extreme are not monitored. However these port links are not prevented form coming up.

The optic parameters that can be monitored are listed and described below.

Table 10: Optic parameter descriptions

SFP parameter	Description	Suggested SFP impact
Temperature	Measures the temperature of the optic, in degrees Celsius.	High temperature suggests that the optic might be damaged.
Receive power (RXP)	Measures the amount of incoming laser, in µWatts.	Describes the condition of the optic. If this parameter exceeds the threshold, the optic is deteriorating.
Transmit power (TXP)	Measures the amount of outgoing laser power, in µWatts.	Describes the condition of the optic. If this parameter exceeds the threshold, the optic is deteriorating.
Current	Measures the amount of current supplied to the optic transceiver.	Indicates hardware failures.
Voltage	Measures the amount of voltage supplied to the optic.	A value higher than the threshold indicates the optic is deteriorating.

For all Extreme certified optics, optical monitoring is performed using Fabric Watch (FW).

Optical monitoring in Fabric Watch

Table 11: Optical monitoring thresholds

SFP type	Default threshold
1GCWDM	1G SFP CWDM
1GLR	1G SFP LR (also used for 1G BXU /BXD SFP)
1GSR	1G SFP SR
10GDWDMT	10G SFP+ DWDM Tunable
10GER	10G SFP+ ER
10GLR	10G SFP+ LR
10GSR	10G SFP+ SR
10GZR	10G SFP+ ZR
10GUSR	10G SFP+ USR
40GESR	40G QSFP+ eSR4 INT
40GLR	40G QSFP+ LR4
40GSR	40G QSFP+ SR4
40GSRINT	40G QSFP+ SR4 INT
40GLM	40G QSFP+ LM4
40GER	40G QSFP+ ER4
100GCLR	100G QSFP28 CLR4
100GCWDM	100G QSFP28 CWDM4

Table 11: Optical monitoring thresholds (continued)

SFP type	Default threshold
100GESR	100G QSFP28 eSR4
100GLR	100G QSFP28 LR4 (For both 4.5W and < 3.5W versions)
100GLRLT	100G QSFP28 LR4 Lite
100GPSM	100G QSFP28 PSM4
100GSR	100G QSFP28 SR4
100GAOC	100G QSFP28 AOC
1GBIDI10KM	1G BX - BiDi SFP 10km
1GBIDI40KM	1G BX - BiDi SFP 40km
1GBIDI120KM	1G BX - BiDi SFP 120km
1GCOP	1G SFP Copper
1GELX	1G ELX SFP
1GFX	1G FX SFP
1GLHA	1G SFP LHA
1GLHB	1G LHB SFP
1GLX	1G LX SFP 10km
1GLX-1	1G LX SFP
1GLXDUAL	1G LX SFP 10km Dual Rate
1GLXTAA	1G LX SFP TAA
1GLXTAA-1	1G LX SFP TAA
1GSX	1G SX SFP
1GSXTAA	1G SX SFP TAA
1GZRCWDM	1G ZR SFP CWDM
1GZRCWDM-1	1G ZR SFP CWDM
1GZRCWDM-2	1G ZR SFP CWDM
8GELS	8G ELS SFP
8GLR	8G LR SFP
8GSR	8G SR SFP
8GSR-1	8G SR SFP
10GBIDI	10G BX - BiDi SFP+ 10km TX
10GBIDI40KM	10G BX - BiDi SFP+ 40km
10GBIDITAA	10G BX - BiDi SFP+ 10km TX TAA
10GCWDM	10G LR SFP+ CWDM
10GCWDM-1	10G LR SFP+ CWDM
10GCWDM-2	10G LR SFP+ CWDM

Table 11: Optical monitoring thresholds (continued)

SFP type	Default threshold
10GDWDMT	10G SFP+ DWDM Tunable
10GER	10G SFP+ ER
10GER40KM	10G ER SFP+ 40km
10GERDWDM	10G ER SFP+ DWDM
10GERDWDM-1	10G ER SFP+ DWDM
10GERX	10G ER XFP
10GET	10GE SFP BaseT
10GLR	10G SFP+ LR
10GLR10KM	10G LR SFP+ 10km
10GLRDUAL	10G LR SFP+ 10km Dual Rate
10GLRDUAL-1	10G LR SFP+ 10km Dual Rate
10GLRMX	10G LRM XFP
10GLRTAA	10G LR SFP+ 10km TAA
10GSLRM	10G LRM SFP+ 220m
10GSLRM-1	10G LRM SFP+
10GSR300M	10G SR SFP+ 300m
10GSR300M-1	10G LRM SFP+
10GSR300M-2	10G LRM SFP+
10GSR300M-3	10G LRM SFP+
10GSRDUAL	10G SR SFP+ Dual Rate
10GSRDUAL-1	10G SR SFP+ Dual Rate
10GSRTAA	1G LX SFP TAA
10GSRTAA-1	1G LX SFP TAA
10GSRX	10G SR XFP
10GUSR	10G SFP+ USR
10GUSR100M	10G USR SFP+ 100m Hight Rx Sens
10GUSR100M-1	10G USR SFP+ 100m
10GUSR100MTA	10G USR SFP+ 100m TAA
10GZR80KM	10GZR80KM
10GZRCWDM	10G ZR SFP+ CWDM
10GZRX	10G ZR XFP
25GER	25G ER SFP28
25GESR	25G ESR SFP28
25GLR	25G LR SFP28 10km

Table 11: Optical monitoring thresholds (continued)

SFP type	Default threshold
25GSR	25G SR SFP28 100m
25GSR100M	25G SR SFP28 100m Lite-FEC
40GSRBIDI	40G SR4 - BiDi QSFP+
100G4WDM	100G 4WDM QSFP28
100GCWDM2KM	100G CWDM4 QSFP28 2km
100GERLT	100G ER4-lite QSFP28
100GLR10KM	100G LR4 QSFP28 10km
100GSR100M	100G SR4 QSFP28 100m
100GSRBIDI	100G SR4 - BiDi QSFP28
100GSWDM	100G SWDM4 QSFP28
100MBIDI	100M BX - BiDi SFP
100MFX	100M FX SFP
100MFX-1	100M FX SFP
100MLX	100M LX SFP

You can customize thresholds and actions for the SFP component using the following commands:

```
device(config)# threshold-monitor sfp policy custom type <type> area <area> [alert|
threshold]
device(config)# threshold-monitor sfp threshold-monitor sfp apply custom
```

You can configure threshold as below or above and configure alert as generating raslog or sending email.

Note
The **show default threshold** command works only on SFP type and not on interface. You can only use policy as **custom**, to customize the thresholds and actions.

Viewing system optical monitoring defaults

The following example command will display the defaults for type 1GLR SFPs:

```
device# show defaults threshold sfp type 1GLR
Type: 1GLR
+------------+-------------------------+-------------------------+--------+
|            |     High Threshold      |     Low Threshold       | Buffer |
| Area       | Value | Above  | Below  | Value     |  Below     | Value  |
|            |       | Action | Action |           |  Action    |        |
+------------+-------+--------+--------+-----------+------------+--------+
| Temp C     |    90 | raslog | none   |        -45|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| RXP uWatts |   501 | raslog | none   |          6|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| TXP uWatts |   794 | raslog | none   |         71|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| Current mA |    45 | raslog | none   |          1|  raslog    |       0|
```

```
+------------+-------+--------+--------+-----------+-------------+--------+
| Voltage mV |  3700 | raslog | none   |       2900|  raslog     |       0|
+------------+-------+--------+--------+-----------+-------------+--------+
device#
```

Viewing the area-wise optical monitoring current status

```
device# show threshold monitor sfp all area temperature
Interface Type Area Value Status
Monitoring Status
-----------------------------------------------------------------
-----------
Eth 0/5 10GSR Temperature 24 Centigrade In Range
Monitoring
```

Tunable SFP+ (T-SFP+) optics

You can specify the desired channel number in the port configuration. Software will program the corresponding wavelength into T-SFP+ EEPROM based on the configuration, when a T-SFP+ is detected. The default factory wavelength of a T-SFP+ is in Zero.

When the T-SFP+ optic module is unplugged, its current programming state is not preserved. When the optic module is re-plugged, the T-SFP+ goes to the default zero wavelength state. When a port configuration is applied, the device is programmed into the desired wavelength state.

To configure a port to the desired channel of T-SFP+, **`tunable-optics sfpp channel`** command is used to configure a port to the desired channel of T-SFP+.

```
device# tunable-optics sfpp channel <channel number (0-102)>
```

Note
Only Extreme recommended channel numbers are accepted. A value of 0 sets the T-SFP+ to the factory default "no wavelength" state.

The **`show media tunable-optic-sfpp`** command displays the optic wavelengths of all Extreme recommended channel numbers. The **`show media tunable-optic-sfpp channel`** command displays the corresponding optic wavelength at the specified Extreme recommended channel number.

Configuring optical monitoring thresholds and alerts

The following is an example of configuring SFP monitoring.

1. Enter global configuration mode.
   ```
   device# configure terminal
   ```
2. Enter **`threshold-monitor sfp`** and create a custom policy.
   ```
   device(config)# threshold-monitor sfp policy custom type 1glr area temperature alert
   above highthresh-action raslog email
   ```
3. Apply the policy.
   ```
   device(config)# threshold-monitor sfp apply custom
   ```

   To disable threshold monitoring, enter the **threshold-monitor**sfp pause command.

   To re-enable monitoring, enter the **`no`** form of the **`threshold-monitor`** command.

Optic thresholds

You can customize Optic thresholds or actions by using the **`threshold-monitor sfp`** command, which enables you to perform the following tasks.

- Customize Optic configurations or accept Optic defaults.
- Manage the actions and thresholds for the Current, Voltage, RXP, TXP, and Temperature areas of the optic.
- Suspend Optical monitoring.

If you do not provide the Optic type parameters, the default thresholds and actions are used. Optic types, monitoring areas, and default threshold values for the 16-Gbps and QSFP optics are detailed below.

Note

- The temperature range specified in the following table is the maximum and minimum operating temperature for that optic. An alarm will be raised if these values are crossed.
- The temperature range specified for the optic in the https://optics.extremenetworks.com portal is the normal operating temperature range for that specific optic. Only RAS logs will be generated if these values are crossed.

Table 12: Factory thresholds for optic types and monitoring areas

Optic type	Area	Unit	Low	High
1GSR	Temperature	C	-40	100
	RX power	uW	8	1122
	TX power	uW	60	1000
	Current	mA	2	12
	Supply voltage	mV	3000	3600
	Power on hours	Hrs	0	0
1GLR	Temperature	C	-45	90
	RX power	uW	6	501
	TX power	uW	71	794
	Current	mA	1	45
	Supply voltage	mV	2900	3700
	Power on hours	Hrs	0	0

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
1GCOP	Temperature	C	-45	90
	RX power	uW	6	501
	TX power	uW	71	794
	Current	mA	1	45
	Supply voltage	mV	2900	3700
	Power on hours	Hrs	0	0
10GUSR	Temperature	C	-5	100
	RX power	uW	32	2000
	TX power	uW	126	2000
	Current	mA	3	11
	Supply voltage	mV	3000	3600
	Power on hours	Hrs	0	0
10GSR	Temperature	C	-5	90
	RX power	uW	32	1000
	TX power	uW	251	794
	Current	mA	4	11
	Supply voltage	mV	3000	3600
	Power on hours	Hrs	0	0
10GLR	Temperature	C	-5	88
	RX power	uW	16	1995
	TX power	uW	158	1585
	Current	mA	15	85
	Supply voltage	mV	2970	3600
	Power on hours	Hrs	0	0
10GER	Temperature	C	-5	75
	RX power	uW	10	1585
	TX power	uW	135	5012
	Current	mA	20	120
	Supply voltage	mV	3035	3665
	Power on hours	Hrs	0	0

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
40GSR	Temperature	C	-5	75
	RX power	uW	40	1995
	TX power	uW	0	0
	Current	mA	1	10
	Supply voltage	mV	2970	3600
	Power on hours	Hrs	0	0
40GSRINT	Temperature	C	-5	75
	RX power	uW	45	2188
	TX power	uW	0	0
	Current	mA	1	55
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
40GESR	Temperature	C	-5	75
	RX power	uW	45	2188
	TX power	uW	0	0
	Current	mA	1	55
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
40GLR	Temperature	C	-5	70
	RX power	uW	21	3380
	TX power	uW	0	0
	Current	mA	5	70
	Supply voltage	mV	2900	3700
	Power on hours	Hrs	0	0
100GSR	Temperature	C	-5	75
	RX power	uW	40	2188
	TX power	uW	100	3162
	Current	mA	3	13
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
100GLR	Temperature	C	-5	75
	RX power	uW	35	3548
	TX power	uW	148	5623
	Current	mA	20	110
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
100GPSM	Temperature	C	0	70
	RX power	uW	55	2818
	TX power	uW	398	2818
	Current	mA	30	70
	Supply voltage	mV	3135	3465
	Power on hours	Hrs	0	0
100GCWDM	Temperature	C	-3	75
	RX power	uW	45	2239
	TX power	uW	114	2818
	Current	mA	5	75
	Supply voltage	mV	3040	3560
	Power on hours	Hrs	0	0
100GCLR	Temperature	C	0	70
	RX power	uW	55	2818
	TX power	uW	398	2818
	Current	mA	30	70
	Supply voltage	mV	3135	3465
	Power on hours	Hrs	0	0
100GLRLT	Temperature	C	-5	75
	RX power	uW	55	3548
	TX power	uW	234	3548
	Current	mA	20	110
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GZR	Temperature	C	-11	91
	RX power	uW	2	51
	TX power	uW	316	3548
	Current	mA	15	130
	Supply voltage	mV	3000	3510
	Power on hours	Hrs	0	0
1GCWDM	Temperature	C	-9	110
	RX power	uW	4	1000
	TX power	uW	398	8310
	Current	mA	2	105
	Supply voltage	mV	2800	4000
	Power on hours	Hrs	0	0
10GDWDMT	Temperature	C	-8	73
	RX power	uW	1	398
	TX power	uW	501	1995
	Current	mA	15	126
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
40GER	Temperature	C	-5	78
	RX power	uW	3	2239
	TX power	uW	0	0
	Current	mA	8	105
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
40GLM	Temperature	C	-5	78
	RX power	uW	17	3388
	TX power	uW	0	0
	Current	mA	8	105
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
100GESR40GLM	Temperature	C	-5	75
	RX power	uW	35	2188
	TX power	uW	74	3467
	Current	mA	2	10
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
100GAOC40GLM	Temperature	C	-5	75
	RX power	uW	40	2188
	TX power	uW	0	0
	Current	mA	3	13
	Supply voltage	mV	2970	3630
	Power on hours	Hrs	0	0
1GBIDI10KM	Temperature	C	-40	95
	RX power	uW	11	501
	TX power	uW	126	501
	Current	mA	3	80
	Supply voltage	mV	2970	3630
1GBIDI40KM	Temperature	C	-40	85
	RX power	uW	6	1000
	TX power	uW	316	1000
	Current	mA	0	300
	Supply voltage	mV	3130	3470
1GBIDI120KM	Temperature	C	-40	85
	RX power	uW	1	200
	TX power	uW	794	2512
	Current	mA	0	500
	Supply voltage	mV	3130	3470
1GELX	Temperature	C	-10	85
	RX power	uW	0	5000
	TX power	uW	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
1GFX	Temperature	C	-40	85
	RX power	uW	0	5000
	TX power	uW	126	794
	Current	mA	0	50
	Supply voltage	mV	2800	4000
1GLHA	Temperature	C	-5	85
	RX power	uW	2	1000
	TX power	uW	794	3981
	Current	mA	2	90
	Supply voltage	mV	3000	3600
1GLHB	Temperature	C	-10	85
	RX power	uW	0	5000
	TX power	uW	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
1GLX	Temperature	C	-40	85
	RX power	uW	5	1585
	TX power	uW	71	794
	Current	mA	0	60
	Supply voltage	mV	3000	3600
1GLX-1	Temperature	C	-40	85
	RX power	uW	10	500
	TX power	uW	100	500
	Current	mA	0	60
	Supply voltage	mV	3000	3600
1GLXDUAL	Temperature	C	-40	95
	RX power	uW	1	158
	TX power	uW	32	158
	Current	mA	3	80
	Supply voltage	mV	2970	3630

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
1GLXTAA	Temperature	C	-40	85
	RX power	uW	10	500
	TX power	uW	100	500
	Current	mA	0	90
	Supply voltage	mV	3000	3600
1GLXTAA-1	Temperature	C	-10	100
	RX power	uW	5	501
	TX power	uW	126	501
	Current	mA	0	90
	Supply voltage	mV	3000	3600
1GSX	Temperature	C	-40	85
	RX power	uW	31	500
	TX power	uW	100	500
	Current	mA	0	50
	Supply voltage	mV	2800	4000
1GSXTAA	Temperature	C	-40	100
	RX power	uW	13	1000
	TX power	uW	158	501
	Current	mA	0	20
	Supply voltage	mV	3000	3600
1GZRCWDM	Temperature	C	-40	85
	RX power	uW	5	1000
	TX power	uW	100	3162
	Current	mA	0	90
	Supply voltage	mV	3000	4000
1GZRCWDM-1	Temperature	C	-40	85
	RX power	uW	5	1000
	TX power	uW	100	3162
	Current	mA	0	90
	Supply voltage	mV	3000	4000

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
1GZRCWDM-2	Temperature	C	-40	85
	RX power	uW	5	1000
	TX power	uW	100	3162
	Current	mA	0	90
	Supply voltage	mV	3000	4000
8GELS	Temperature	C	-10	85
	RX power	uW	12	1122
	TX power	uW	250	2500
	Current	mA	0	50
	Supply voltage	mV	2800	4000
8GLR	Temperature	C	-10	85
	RX power	uW	12	1122
	TX power	uW	144	1122
	Current	mA	0	50
	Supply voltage	mV	2800	4000
8GSR	Temperature	C	-40	125
	RX power	uW	10	1000
	TX power	uW	100	1585
	Current	mA	0	20
	Supply voltage	mV	2800	4000
8GSR-1	Temperature	C	-10	85
	RX power	uW	49	500
	TX power	uW	100	500
	Current	mA	0	20
	Supply voltage	mV	2800	4000
10GBIDI	Temperature	C	-40	85
	RX power	uA	36	1122
	TX power	uA	151	1122
	Current	mA	0	65
	Supply voltage	mV	3100	3500

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GBIDI40KM	Temperature	C	-40	125
	RX power	uA	40	1122
	TX power	uA	1585	5012
	Current	mA	0	285
	Supply voltage	mV	3130	3470
10GBIDITAA	Temperature	C	-40	125
	RX power	uA	40	1122
	TX power	uA	316	1000
	Current	mA	0	400
	Supply voltage	mV	3130	3470
10GCWDM-1	Temperature	C	-10	75
	RX power	uA	10	1585
	TX power	uA	316	1585
	Current	mA	0	20
	Supply voltage	mV	2800	4000
10GCWDM-2	Temperature	C	-10	75
	RX power	uA	10	1585
	TX power	uA	316	1585
	Current	mA	0	20
	Supply voltage	mV	2800	4000
10GER40KM	Temperature	C		
	RX power	uA	-10	85
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
10GERDWDM	Temperature	C	-8	73
	RX power	uW	20	1000
	TX power	uW	501	3162
	Current	mA	40	120
	Supply voltage	mV	3000	3600

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GERDWDM -1	Temperature	C	-8	73
	RX power	uA	20	1000
	TX power	uA	501	3162
	Current	mA	40	120
	Supply voltage	mV	3000	3600
10GERX	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
10GET	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
10GLR10KM	Temperature	C	-5	70
	RX power	uA	38	1122
	TX power	uA	151	1122
	Current	mA	0	20
	Supply voltage	mV	3100	3500
10GLRDUAL	Temperature	C	-40	125
	RX power	uA	6	1585
	TX power	uA	100	1585
	Current	mA	0	20
	Supply voltage	mV	2800	4000
10GLRDUAL -1	Temperature	C	0	70
	RX power	uA	25	1120
	TX power	uA	151	1120
	Current	mA	0	20
	Supply voltage	mV	2800	4000

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GLRMX	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
10GLRTAA	Temperature	C	-10	90
	RX power	uA	16	1259
	TX power	uA	126	1413
	Current	mA	7	100
	Supply voltage	mV	3000	3600
10GSLRM	Temperature	C	-40	125
	RX power	uA	6	1000
	TX power	uA	100	1995
	Current	mA	0	75
	Supply voltage	mV	2800	4000
10GSLRM-1	Temperature	C	-25	95
	RX power	uA	10	1259
	TX power	uA	158	1585
	Current	mA	2	90
	Supply voltage	mV	2800	3800
10GSR300M	Temperature	C	0	70
	RX power	uA	10	1000
	TX power	uA	126	562
	Current	mA	0	20
	Supply voltage	mV	3140	3460
10GSR300M-1	Temperature	C	-10	85
	RX power	uA	77	500
	TX power	uA	100	500
	Current	mA	0	20
	Supply voltage	mV	3140	3460

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GSR300M-2	Temperature	C	-20	90
	RX power	uiA	10	1259
	TX power	uA	160	1589
	Current	mA	1	20
	Supply voltage	mV	2800	3000
10GSR300M-3	Temperature	C	-5	70
	RX power	uA	10	1000
	TX power	uA	126	562
	Current	mA	0	20
	Supply voltage	mV	3000	3600
10GSRDUAL	Temperature	C	-40	125
	RX power	uA	˜10	1000
	TX power	uA	100	794
	Current	mA	0	20
	Supply voltage	mV	2800	4000
10GSRDUAL-1	Temperature	C	-10	85
	RX power	uA	77	500
	TX power	uA	100	500
	Current	mA	0	20
	Supply voltage	mV	2800	4000
10GSRTAA	Temperature	C	-10	85
	RX power	uA	77	500
	TX power	uA	100	500
	Current	mA	1	20
	Supply voltage	mV	2800	4000
10GSRTAA-1	Temperature	C	-20	90
	RX power	uA	10	1259
	TX power	uA	160	1589
	Current	mA	1	20
	Supply voltage	mV	2800	3000

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GSRX	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
10GUSR	Temperature	C	-5	100
	RX power	uA	32	2000
	TX power	uA	126	2000
	Current	mA	3	11
	Supply voltage	mV	3000	3600
10GUSR100M	Temperature	C	-5	85
	RX power	uA	10	1000
	TX power	uA	316	794
	Current	mA	0	20
	Supply voltage	mV	3140	3460
10GUSR100M-1	Temperature	C	-10	85
	RX power	uA	77	500
	TX power	uA	100	500
	Current	mA	0	20
	Supply voltage	mV	3140	3460
10GUSR100MTA	Temperature	C	-5	70
	RX power	uA	10	1000
	TX power	uA	126	562
	Current	mA	0	20
	Supply voltage	mV	3140	3640
10GZR	Temperature	C	-11	91
	RX power	uA	2	251
	TX power	uA	316	3548
	Current	mA	15	130
	Supply voltage	mV	3000	3510

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
10GZR80KM	Temperature	C	-10	75
	RX power	uA	2	316
	TX power	uA	794	3162
	Current	mA	0	127
	Supply voltage	mV	2800	4000
10GZRCWDM	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
10GZRX	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
25GER	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
25GESR	Temperature	C	0	70
	RX power	uA	79	1738
	TX power	uA	126	1738
	Current	mA	0	50
	Supply voltage	mV	3140	3450
25GLR	Temperature	C	0	70
	RX power	uA	52	1585
	TX power	uA	200	1585
	Current	mA	0	300
	Supply voltage	mV	3135	3465

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
25GSR	Temperature	C	0	70
	RX power	uA	79	1738
	TX power	uA	126	1738
	Current	mA	0	50
	Supply voltage	mV	3140	3450
25GSR100M	Temperature	C	0	85
	RX power	uA	40	1000
	TX power	uA	158	794
	Current	mA	0	20
	Supply voltage	mV	3150	3460
40GSRBIDI	Temperature	C	10	70
	RX power	uW	170	1000
	TX power	uW	0	0
	Current	mA	0	50
	Supply voltage	mV	2800	4000
40GSRINT	Temperature	C	-5	75
	RX power	uA	45	2188
	TX power	uA	0	0
	Current	mA	1	55
	Supply voltage	mV	2970	3630
100G4WDM	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
100GCWDM2KM	Temperature	C	0	70
	RX power	uA	71	1778
	TX power	uA	224	1778
	Current	mA	0	100
	Supply voltage	mV	0	3450

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
100GERLT	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
100GLR10KM	Temperature	C	0	70
	RX power	uA	87	2818
	TX power	uA	372	2818
	Current	mA	0	100
	Supply voltage	mV	0	3465
100GLRLT	Temperature	C	-5	75
	RX power	uA	55	3548
	TX power	uA	234	3548
	Current	mA	20	110
	Supply voltage	mV	2970	3630
100GSR100M	Temperature	C	-10	80
	RX power	uA	40	3467
	TX power	uA	62	3467
	Current	mA	0	12
	Supply voltage	mV	3000	3600
100GSRBIDI	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
100GSRBIDI	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000

Table 12: Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
100MBIDI	Temperature	C	-40	95
	RX power	uA	1	40
	TX power	uA	40	158
	Current	mA	3	80
	Supply voltage	mV	2970	3630
100MFX	Temperature	C	-40	85
	RX power	uA	62	125
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
100MFX-1	Temperature	C	-10	85
	RX power	uA	0	5000
	TX power	uA	0	5000
	Current	mA	0	50
	Supply voltage	mV	2800	4000
100MLX	Temperature	C	-40	95
	RX power	uA	1	200
	TX power	uA	25	200
	Current	mA	0	80
	Supply voltage	mV	3000	3600

Threshold values

A combination of high and low threshold settings can cause the following actions to occur:

- Above high threshold — A default or user-configurable action is taken when the current value is above the high threshold.
- Below high threshold — A default or user-configurable action is taken when the current value is between the high and low threshold.
- Below low threshold — A default or user-configurable action is taken when the current value is below the low threshold.
- Above low threshold — monitoring is not supported for this value.

Disk space monitoring and management

Disk space on SLX-OS devices is limited and is partitioned for optimal use. As the device runs, a number of log files are generated along with core-dump files when a process crashes for any reason. Over a period of time, these logs and core-dump files consume space on the device's HDDs and could cause various issues with the device's stability and availability.

From SLX-OS version 20.7.2, the */root* and */support* partitions are periodically monitored (at 10 minute intervals) for available free space. As log files and core-dump files accumulate, the amount of free space reduces. When the available free space goes below the pre-defined threshold of 1024 MB, an alarm is generated. Subsequent alarms are generated for every 100 MB of space being consumed.

Once every monitoring cycle of 10 minutes the core-dump files, stored in the `/core_files/misc-cores` directory, are cleared. For each process, three latest core-dump files are retained. Older files are discarded.

Also, for every cleanup cycle, a new log file, `misc_core_del.log` is generated and stored in the `/var/log` directory. This log file contains a detailed summary of all scanned files including their timestamp, and names. Core-files that were deleted are clearly identified in this log file. This log file is included as a part of *Support Save*.

Port Monitoring

SLX-OS' Port Monitoring module periodically monitors the ports installed on the device. It uses I2C requests to read the EEPROM and the CPLD of the pluggable media or pluggable port.

This module detects an issue with a port when it is unable to read the EEPROM using I2C. These I2C requests may fail if there are issues with the port's hardware/firmware.

Another reason of the cause of an I2C error is the failure of the I2C controller itself. When the controller itself encounters an error, the Port Monitoring module will be unable to read the status of the various ports, causing the device to mark these ports as being offline.

When I2C errors are encountered, the Port Monitoring module marks the affected ports as *removed*. This causes loss of traffic on the device.

This topic discusses how I2C errors are handled by SLX-OS and how the affected device is gracefully shutdown or taken offline by the software.

Types of I2C Errors

The following are the types of I2C errors that can be encountered:

- **EEPROM I2C Errors** - These errors are mainly caused by hardware failure of the pluggable media or pluggable port. These failures are not recoverable by a *reload* or a *power-cycle* of the SLX-OS device. The SLX-OS device can only be recovered when the ports experiencing these errors are either removed or replaced.
- **CPLD I2C Errors** - These errors are recoverable by *reloading* or *power-cycling* the SLX-OS device. However, reload/power-cycle should only be performed when the pluggable media or pluggable port causing *EEPROM I2C Errors* are removed or replaced.

I2C Errors on MCT Clusters

In a MCT cluster, SLX-OS always uses *active-active* forwarding mode. When using this mode, on encountering an error, if the MCT Client port is not removed, the multihomed client/access device is unable to detect this fault and is unable to re-route the traffic through the MCT peer. This causes traffic loss.

In the MCT cluster, the role the node plays - *primary* or *secondary* - determines which node will forward traffic to avoid traffic duplication in the case of *Split-Brain* scenario.

Split-Brain is the state, where, in the MCT Cluster, the communication between the MCT peers is down (Inter Chassis Link down) but the MCT Keep Alive (through out of band channels) is up. To avoid forwarding issues during this scenario,the *Client Isolation Mode* is activated where the *Primary* node forwards all the traffic while the *Secondary* node brings down all the client interfaces. In this scenario, an I2C error occurring on the *Primary* node, will result in the traffic being black-holed.

Handling I2C Errors on MCT Clusters

I2C errors cause traffic disruptions on MCT Clusters and must be gracefully handled by the nodes of the MCT Cluster.

Ports with I2C errors must be forcefully shutdown to cause the link to go out of synchronisation. Shutdown of the port turns off the LASER and the transmitter of the affected port. As the port is turned off, it allows the connected device to detect the loss of synchronisation, and, consequently, redirect the traffic to other active ports.

Depending on the number of ports affected due to I2C errors, the SLX-OS software might decide to, either, shutdown the ports with I2C errors, or, put the SLX-OS device in *Maintenance Mode* (MM).

Handling MCT Failure Scenarios

The following is a list of MCT failure scenarios and how they are handled.

- **Port Channel Member Failure :** If the affected port is a member of a Port Channel and the other members of the same Port Channel are active, MCT continues to operate normally, but with reduced bandwidth. Since both MCT nodes run in *active-active* mode, traffic is not expected to be impacted in the normal course. Additional resiliency mechanisms are not triggered until the last member port in the Port Channel goes down.
- **ICL Port Failure :** If the affected port is the last active member of a Inter Chassis Link (ICL), the SLX-OS software transitions the device to *Maintenance Mode* (MM). This takes the affected MCT node out of service. Since the MCT node is not available, traffic switches seamlessly to the MCT peer node. However, this causes a loss of redundancy as only one node is available and in use.
- **Cluster Track or other Cluster Edge Port (CEP) Failures :** If the affected port is a Cluster Edge Port or a Cluster Track Port, then MCT continues to function normally and the affected port is shutdown to maintain stability in the network.
- **Cluster Client Port (CCEP) Failure :** If the affected port is a CCEP, the Port Monitoring module, shuts down the port to allow the connected client device to detect the loss of synchronisation and transition the traffic to the peer MCT node.
- **Widespread Port Failures (when greater than 50% of Cluster Ports Fail) :** If, on the SLX-OS device, more that 50% of the Cluster Client or Cluster Track ports are affected simultaneously. This indicates a major hardware issue which could also lead to additional

faults in the future. In this case, the SLX-OS software forces the device into *Maintenance Mode* (MM) to prevent further disruptions to the network.

Caution

Do not attempt to re-enable a port that is shutdown due to an I2C error or as a part of a device that is put into *Maintenance Mode* through the device's CLI or through XCO.

Do not attempt to disable *Maintenance Mode* once it is enabled on a node by the SLX-OS software.

It is recommended that, after removing and/or replacing the affected pluggable media or pluggable port, the device be re-booted manually.

Cyclic redundancy check (CRC)

If the number of CRC error exceeds the configured threshold in a polling window, the configured action is taken. You can set the threshold in the range 1 to 10.

Note

This feature is enabled by default. The default threshold is 5.

Port CRC supports following actions:

- **Raslog**: This is configured by default and the event are logged.
- **Port-shutdown**: If port-shutdown is configured as action, the event is logged and the port shuts down. The interface state changes to port CRC down. To bring up the port, you must explicitly enable the port.

The port CRC is enabled using the **`crc enable`** command. The command is run from the system monitor port configuration mode.

```
device (config-sys-mon-port)# crc ?
Possible completions:
  action          Set Port CRC Monitoring Action
  enable          Enable Port CRC Monitoring (Default: Enabled)
  poll-interval   Set Port CRC Monitoring Poll-Interval
  threshold       Set Port CRC Monitoring Threshold
```

The command **`crc action`** allows you to set various actions. The command **`crc poll-interval`** allows you to set the polling interval. The command **`crc threshold`** allows you to set the crc monitoring threshold.

The **`show interface status`** command displays the port crc status.

```
device# show interface status
--------------------------------------------------------------------------------
Port         Status          Mode       Speed    Type            Description
--------------------------------------------------------------------------------
Eth 3/1      connected (up)  --         10G      10G-SFP-SR
Eth 3/2      adminDown       --         --       --
Eth 3/3      notconnected    --         --       10G-SFP-SR
Eth 3/4      port-crcDown    --         --       --
```

To view port crc status on a specific ethernet interface, issue the **show interface ethernet** command.

```
device# show interface ethernet 3/4
Ethernet 3/4 is port-CRC down, line protocol is down (port-crc down)
Hardware is Ethernet, address is 00e0.0c76.79e8
    Current address is 00e0.0c76.79e8
Pluggable media not present
Interface index (ifindex) is 415367190
MTU 1548 bytes
10G Interface
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Last clearing of show interface counters: 13:19:17
Queueing strategy: fifo
Receive Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Bro
```

You can also view the port crc status by issuing the **show ip interface brief** command.

```
device# show ip interface brief

Interface              IP-Address          Vrf
Status                    Protocol
==================     ==========          ==================
====================      ========
Port-channel 1         unassigned                                administratively
down     down
Port-channel 2         unassigned                                administratively
down     down
Ethernet 3/1           10.3.1.1            default-vrf
up                        up
Ethernet 3/2           unassigned          default-vrf             port-crc
down             down
Ethernet 3/3           10.3.3.1            default-vrf
up                        down
Ethernet 3/4           unassigned          default-vrf             administratively
down     down
```

To view the port crc status on a specific ip interface, issue the **ip interface ethernet** command.

```
device# show ip interface ethernet 3/4
 Ethernet 3/4 is port-crc down protocol is down
 IP unassigned
 Proxy Arp is not Enabled
 Vrf : default-vrf
```

High and Low watermarks for port utilization

Overview

This helps in monitoring and analyzing bandwidth usage and route traffic patterns, allowing you to capture burst conditions by tracking high and low water marks.

Note
This feature is applicable only for Ethernet ports.

This features uses the snapshot of the ethernet port statistics maintained in the management module (MM). The statistics is updated periodically. This data is used to update the high and low water mark values. When the system is up, all the watermark values are set to zero by default.

Recording high and low water marks

This feature reads the ethernet port statistics in every 6 seconds and collects the ingress and egress MBPS and PPS. If the collected value is greater than the existing high watermark value, the high watermark value is updated with the collected value. If the value is non-zero and lower than the existing low watermark value, the low watermark value is updated with the collected value. If the value is zero, then it is ignored.

The watermark values recorded are maintained in two ways; the last 2 hours and the last two days.

- The last two hours data is maintained in two windows – the current one hour and the last one hour. When the current one hour expires, the last one hour data is updated with the recently expired current one hour data and a new current one hour window is opened.
- The last 2 days data is maintained in two windows – The current 24 hours and the last 24 hours. When the current 24 hours expire, the last 24 hours data is updated with the recently expired current 24 hours data and a new current 24 hours window is opened.



Note
The current 1 hour and 24 hour windows start when the MM is up.

Resetting watermark values

The watermark values are reset on chassis reboot. If a card goes down, the values for that card is maintained just the in the way it is handled when the card is up. Whenever a new card is up, watermark feature checks if the new card type is different from the old card that was occupying the slot. If yes, the data for that particular slot is reset.

Enabling and disabling High and Low watermarks

You can enable the high and low watermark feature using the **system interface utilization-watermark** command. The command is run form the configuration mode.

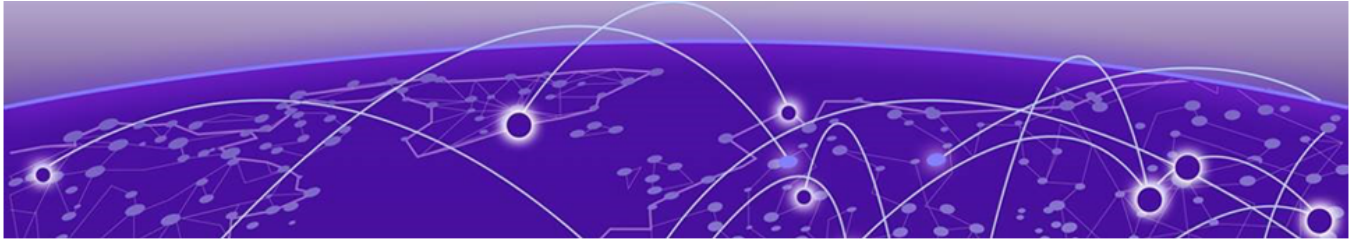
```
device(config)# system interface utilization-watermark
```

The no form of the command disables the feature. For more details about the command, please refer the SLX-OS Command Reference guide.



Note
By default, this feature is enabled globally.

When the feature is disabled, the watermark values already recorded persist. When the feature is enabled again, all the watermark values are reset to default. The **show** and **clear** commands to display and clear watermark values are available even when the feature is disabled. When you disable the feature, the configuration shall be saved and restored on reset.



Remote Monitoring

RMON overview on page 100
Configuring and managing RMON on page 100

RMON overview

Remote monitoring (RMON) is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Configuring and managing RMON

Both alarms and events are configurable RMON parameters.

- Alarms allow you to monitor a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms are paired with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Events determine the action to take when an event is triggered by an alarm. The action can be to generate a log entry, an SNMP trap, or both. You must define the events before an alarm can be configured. If you do not configure the RMON event first, you will receive an error when you configure the alarm settings.

By default, no RMON alarms and events are configured and RMON collection statistics are not enabled.

Configuring RMON events

You can add or remove an event in the RMON event table that is associated with an RMON alarm number.

To configure RMON events, perform the following steps from privileged EXEC mode.

1. Enter the **configure terminal** command to access global configuration mode.

```
device# configure terminal
```

2. Configure the RMON event for generating logs and traps.

```
device(config)# rmon event 27 description Rising_Threshold log owner    john_smith
trap syslog
```

3. Return to privileged EXEC mode.

```
device(config)# end
```

4. Save the *running-config* file to the *startup-config* file.

```
device# copy running-config startup-config
```

Configuring Message Rate Limiting Constraints for Threshold Monitoring

An event can cause multiple messages of different types to be generated simultaneously.

Since it is possible that multiple entries/traps can be generated for an event, options are available to rate limit the generation of these events/traps. Without rate limiting, there is a possibility that the message handling subsystem of the device getting overwhelmed while handling these messages and causing the device to crash.

Rate limiting consists of two configurable constraints:

- the number of messages (X)
- the duration (Y) (in seconds)

When configured, the constraints can be summed as: *Generate a maximum of X messages in Y units of time*. Messages can be RASLOG or SNMP or Both and this depends on the *action* configured for that specific monitored parameter.

To configure the rate limiting constraints:

1. Navigate to the Global Configuration Mode.

```
SLX# configure terminal
SLX (config)#
```

2. Set the *count* parameter.

```
SLX (config)# threshold-monitor hardware-resources count 10
SLX (config)#
```

   The *count* controls the maximum number of events to be generated in the configured time interval. A maximum number of sixty (60) events can be generated for each time interval. The default is four (4).

3. Set the *interval* parameter.

```
SLX (config)# threshold-monitor hardware-resources interval 300
SLX (config)#
```

   The *interval* controls the time duration in seconds. In this example, a maximum of 10 messages can be generated every 300 seconds. The range is 30-900 seconds and the default is 30 seconds.

This example shows the complete configuration for the rate limiting constraints.

```
SLX# configure terminal
SLX (config)# threshold-monitor hardware-resources count 10
SLX (config)# threshold-monitor hardware-resources interval 300
SLX (config)#
```

Configuring RMON alarm settings

To configure RMON alarms and events, perform the following steps from privileged EXEC mode.

1. Enter the **configure terminal** command to access global configuration mode.

```
device# configure terminal
```

2. Configure the RMON alarms.

   Example of an alarm that tests every sample for a rising threshold

```
device(config)# rmon alarm 5 1.3.6.1.2.1.16.1.1.1.5.65535 interval 30
                        absolute rising-threshold 95 event 27 owner john_smith
```

   Example of an alarm that tests the delta between samples for a falling threshold

```
device(config)# rmon alarm 5 1.3.6.1.2.1.16.1.1.1.5.65535 interval 10 delta
                        falling-threshold 65 event 42 owner john_smith
```

3. Return to privileged EXEC mode.

```
device(config)# end
```

4. Save the *running-config* file to the *startup-config* file.

```
device# copy running-config startup-config
```

5. To view configured alarms, use the **show running-config rmon alarm** command.

Monitoring CRC errors

The following synchronizes the statistics maintained for the interface and RMON, as well as ensures proper reporting from an operational standpoint.

1. Issue the **clear counters all** command in global configuration mode.

```
device# clear counters all
```

2. Issue the **clear counters rmon** command.

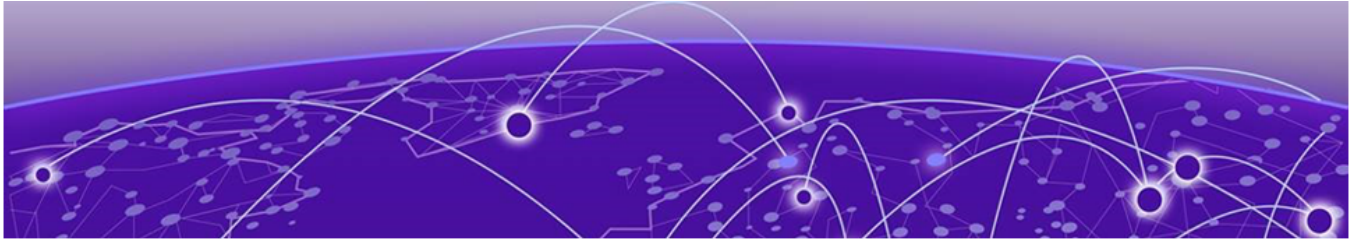
```
device# clear counters rmon
```

3. Execute the **rmon collection stats** command on each interface, as in the following example.

```
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# rmon collection stats 2 owner admin
```

4. Use an appropriate RMON MIB for additional monitoring.

   For example, to obtain CRC statistics on a Extreme SLX-OS platform, the following RMON MIB could be used: Object-etherStatsCRCAlignErrors, OID- .1.3.6.1.2.1.16.1.1.1.8



System Monitoring

System Monitor overview on page 103
Configuring System Monitor on page 106

System Monitor overview

Because of platform-specific values that vary from platform to platform, it was previously not possible to configure platform-specific thresholds through a global CLI command.

Threshold and notification configuration procedures are described in the following sections.

Monitored components

The following FRUs and temperature sensors are monitored on supported devices:

- compact-flash—Displays the threshold for the compact flash device.
- fan—Configures fan settings.
- power—Configures power supply settings.
- temp—Displays the threshold for the temperature sensor component.

Monitored FRUs

System Monitor monitors the absolute state of the following FRUs:

- Fan
- Power supply
- CID card
- SFM

Possible states for all monitored FRUs are removed, inserted, on, off, and faulty. A state of none indicates the device is not configured. If the FRU is removed, inserted, or goes into a faulty state, System Monitor sends a RASLog message or an e-mail alert, depending on the configuration. The health status of the FRU being monitored is not affected by the on or off status. The System Monitor generates a separate RASLog message for the overall health of the device. Use the **`show system monitor`** command to view the health status of a device. Refer to the *Displaying the device health status* section for example output.

SFM monitoring

FE Health Monitoring

All SFM-FEs are periodically polled to check for any access issues. When the number of error events in a polling window crosses the threshold, action is taken. You can configure the parameters using the **sysmon fe-access-check** command.

```
device(config)# sysmon fe-access-check ?
Possible completions:
  action               Set Fe-Access-Check action
  disable              Disable Fe Access Check (Default: Enabled)
  poll-interval        Set Fe-Access-Check poll-interval
  recovery-threshold   Set Fe-Access-Check recovery threshold
  threshold            Set Fe-Access-Check threshold
device(config)#
```

SFM Walk

This algorithm tries to isolate an SFM-FE in case of egress TM reassembly errors. It disables an SFM-FE, monitors egress TM reassembly errors and then either isolates it or re-enables it before moving on to next SFM-FE. This can be triggered manually or by egress monitoring running on TMs. You can configure the parameters using the **sysmon sfm-walk** command.

```
device(config)# sysmon sfm-walk ?
Possible completions:
  auto                       Enable Auto SFM Walk (Default: Disabled)
  disable-redundancy-check   Disable SFM Walk redundancy check (Default:
                             Enabled)
  poll-interval              Set SFM Walk poll-interval
  threshold                  Set SFM Walk reassembly error threshold
device(config)#
```

Use the **sysmon sfm-walk** command to manually start or stop SFM walk.

```
device# sysmon sfm-walk ?
Possible completions:
  start   Start SFM Walk
  stop    Stop SFM Walk
device#
```

FE Link CRC Monitoring

All SFM-FE and TM fabric links are polled periodically to check for slow CRC errors. When the number of CRC events in a window crosses threshold, action is taken. You can configure the parameters using the **sysmon link-crc-monitoring** command.

```
device(config)# sysmon link-crc-monitoring ?
Possible completions:
  action          Set Link CRC Monitoring action
  disable         Disable Link CRC Monitoring (Default: Enabled)
  poll-interval   Set Link CRC Monitoring poll-interval
  threshold       Set Link CRC Monitoring threshold
device(config)#
```

Show commands

Following are sample show command outputs for the SFM module.

```
device# show sfm ?
Possible completions:
  link-connectivity   Display fabric connectivity
  link-thresholds     Display fabric thresholds
  links               Display fabric links
  mcast               Display fabric mcast entries
  queue-occupancy     Display fabric queues
```

```
  serdes-mode         Display fabric serdes-mode
  statistics          Display fabric global counters
device# show sfm link-connectivity
SFM Connectivity (FE 4):
--------------------
Link | Logical Port | Remote Module | Remote Link | Remote Device Type
-------------------------------------------------------------------------
036  |     036      |     0012      |     011     |     FAP
037  |     037      |     0012      |     009     |     FAP
038  |     038      |     0012      |     010     |     FAP
039  |     039      |     0012      |     008     |     FAP
device# show sfm queue-occupancy
FE Queue (FE 4):
DCH Queues:
=========
DCH0 Pipe 0: [22,9]
DCH1 Pipe 0: [59,6]
DCH2 Pipe 0: [64,8]
DCH3 Pipe 0: [136,6]

DCL Queues:
=========
DCL0 Pipe 0: [20,4]
DCL1 Pipe 0: [56,12]
DCL2 Pipe 0: [136,4]
device# show sfm link-thresholds
   Link |   Pipe       |     GCI1      |      GCI2   |   GCI2
   RX Thresholds:
   001  |     000      |     0511      |     511     |   511
   TX Thresholds:
   001  |     000      |     0024      |     032     |   40
device# show sfm links
FE-LINKS:
FE Links (FE 4):
 Link  | CRC Error | Size Error | Code Group Error | Misalign | No Signal Lock | No
signal accept | Errored tokens | Errored tokens count

-------------------------------------------------------------------------------------------
-----------------------------------------------
  0    |    -      |     -      |   ***    |      ***       |        ***         |
***       |    ***         |  0
  1    |    -      |     -      |   ***    |      ***       |        ***         |
***       |    ***         |  0
  2    |    -      |     -      |   ***    |      ***       |        ***         |
***       |    ***         |  0
  3    |    -      |     -      |   ***    |      ***       |        ***         |
***       |    ***         |  0
  4    |    -      |     -      |   -      |      -         |        -           |
-         |     -          |  63
  5    |    -      |     -      |   -      |      -         |        -           |
-         |     -          |  63
  6    |    -      |     -      |   -      |      -         |        -           |
-         |     -          |  63
device# show sfm mcast id 1
For MGID 1 fap-list: idx:1 fap-id:0x0
For MGID 1 fap-list: idx:2 fap-id:0x1
For MGID 1 fap-list: idx:3 fap-id:0x2
For MGID 1 fap-list: idx:4 fap-id:0x3
device# show sfm statistics
#-------------------------------------------------------------------------#
#                          |                  Pipe 0                     #
#-------------------------------------------------------------------------#
```

```
# DCH:                      |                                          #
#     Total Incoming Cells |                    0                      #
#     Total Outgoing Cells |                    0                      #
#     Fifo Discard         |                    0                      #
#     Reorder Discard      |                    0                      #
#     Unreach Discard      |                    0                      #
#     Max Cells in Fifos   |                    0                      #
#-----------------------------------------------------------------------#
#-----------------------------------------------------------------------#
# DCM:                      |                                          #
#     Total Incoming Cells |                    0                      #
#     Dropped Cells        |                    0                      #
#     Max Cells in Fifos   |                    0                      #
#-----------------------------------------------------------------------#
#-----------------------------------------------------------------------#
# DCL:                      |                                          #
#     Total Incoming Cells |                    0                      #
#     Total Outgoing Cells |                    0                      #
#     Dropped Cells        |                    0                      #
#     Max Cells in Fifos   |                    0                      #
#-----------------------------------------------------------------------#
#-----------------------------------------------------------------------#
device# show switch_fabric_module

Slot  Type         Description                 ID      Status
---------------------------------------------------------------------
S1   SFM8 v6      Switch Fabric Module        187     ENABLED
S2   SFM8 v6      Switch Fabric Module        187     ENABLED
S3   SFM8 v6      Switch Fabric Module        187     ENABLED
S4   SFM8 v6      Switch Fabric Module        187     ENABLED
S5   SFM8 v6      Switch Fabric Module        187     ENABLED
S6   SFM8 v6      Switch Fabric Module        187     ENABLED
```

Configuring System Monitor

This section contains example basic configurations that illustrate various functions of the **`system-monitor`** command and related commands. For CLI details, refer to the *Command Reference* for your product.

Setting system thresholds

Each component can be in one of two states, down or marginal, based on factory-defined or user-configured thresholds. (The default thresholds are listed in Configuring System Monitor on page 106.)

1. Issue the **`configure terminal`** command to enter global configuration mode.
2. Change down-threshold and marginal-threshold values for the Fan.

```
device(config)# system-monitor fan threshold marginal-threshold 1 down-threshold 2
```



Note
You can disable the monitoring of each component by setting down-threshold and marginal-threshold values to 0 (zero).

Setting state alerts and actions

System Monitor generates an alert when there is a change in the state from the default or defined threshold.

1. Issue the **configure terminal** command to enter global configuration mode.
2. To enable a RASLog alert (example: when the power supply is removed), enter the following command:

```
device(config)# system-monitor power alert state removed action raslog
```

Note
There are no alerts for MM, compact-flash, or temp. There are no alert actions for SFPs.

Configuring e-mail alerts

Use the **system-monitor-mail fru** command to configure e-mail threshold alerts for FRU and optic monitoring. For an e-mail alert to function correctly, you must add the IP addresses and host names to the domain name server (DNS) in addition to configuring the domain name and name servers. For complete information on the **system-monitor-mail relay host** command, refer to the *Extreme SLX-OS Command Reference Guide*.

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter the following command to enable e-mail alerts and to configure the e-mail address.

```
device(config)# system-monitor-mail fru enable email-id
```

Sendmail agent configuration

The sendmail agent must have one of the following configuration to resolve the domain-name.

- Configure DNS settings to connect device to DNS server.
- In case if DNS server is not available, DNS configuration along with relay host configuration is required for the sendmail agent on the device to resolve the domain-name. E-mail can be forwarded through the relay host. For example:

```
device(config)# ip dns domain-name domain_name1.Extreme.com
device(config)# ip dns name-server 1.2.3.4
device(config)# ip dns name-server 1.2.3.4
```

The following **system-monitor-mail relay host** commands allow the sendmail agent on the device to resolve the domain name and forward all e-mail messages to a relay server.

- To create a mapping:
- To delete the mapping:
- To change the domain name:

Note
You must delete the first domain name before you can change it to a new domain name.

- To delete the domain name and return to the default:

Viewing system optical monitoring defaults

The following example command will display the defaults for type 1GLR SFPs:

```
device# show defaults threshold sfp type 1GLR
Type: 1GLR
+------------+------------------------+------------------------+--------+
|            |     High Threshold     |     Low Threshold      | Buffer |
| Area       | Value | Above  | Below | Value     |  Below     | Value  |
|            |       | Action | Action|           |  Action    |        |
+------------+-------+--------+-------+-----------+------------+--------+
| Temp C     |    90 | raslog | none  |        -45|  raslog    |       0|
+------------+-------+--------+-------+-----------+------------+--------+
| RXP uWatts |   501 | raslog | none  |          6|  raslog    |       0|
+------------+-------+--------+-------+-----------+------------+--------+
| TXP uWatts |   794 | raslog | none  |         71|  raslog    |       0|
+------------+-------+--------+-------+-----------+------------+--------+
| Current mA |    45 | raslog | none  |          1|  raslog    |       0|
+------------+-------+--------+-------+-----------+------------+--------+
| Voltage mV |  3700 | raslog | none  |       2900|  raslog    |       0|
+------------+-------+--------+-------+-----------+------------+--------+
device#
```

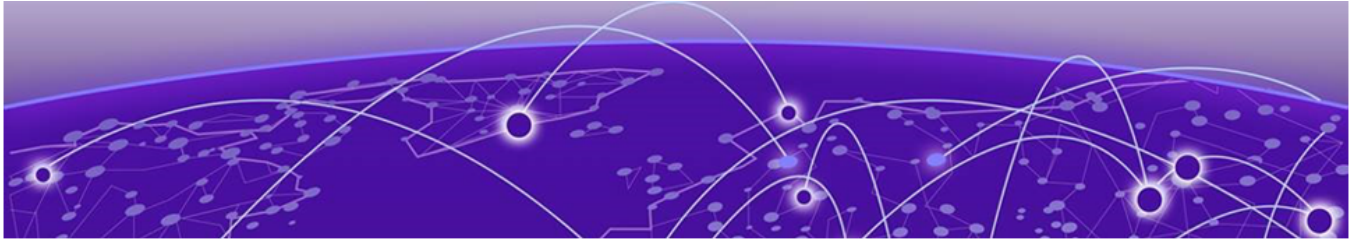
Viewing the area-wise optical monitoring current status

```
device# show threshold monitor sfp all area temperature
Interface                              Type            Area            Value
Status        Monitoring Status
-------------------------------------------------------------------------------------------------
------------------------------
Eth 0/5                                10GSR           Temperature     24 Centigrade
In Range      Monitoring
```

Displaying the device health status

To display the health status of a device, enter **show system monitor**.

```
SLX# show system monitor
** ** System Monitor Switch Health Report **
                Switch status            : MARGINAL
                Time of Report           : 2020-01-05 01:05:39
                Power supplies monitor   : MARGINAL
                Temperatures monitor     : HEALTHY
                Fans monitor             : HEALTHY
                Flash monitor            : HEALTHY
SLX#
```



Logging and tracing

Overview on page 109
RASLog on page 109
AuditLog on page 110
Syslog on page 111

Overview

RASTrace captures low level info which can be used for debugging or troubleshooting issues. Use the **rasdecode** command to decode the traces collected. You must provide the module ID (-m) and display count (-n) parameters.

Use the tracecfg command to display, clear, and modify the trace configurations such as debug level, number of trace entries, trace dump size, and so on, for any individual module. Use tracecfg -h command from the linux shell for usage information.

RASTrace, RASLog, AuditLog, and Syslog are detailed in the following section of the docuemnt.

RASLog

It can store 2048 external customer visible messages in total. These are forwarded to the console, to the configured syslog servers and through the SNMP traps or informs the SNMP management station.

There are four levels of severity for messages, ranging from CRITICAL to INFO. In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. You must look at each specific error message description thoroughly before taking action.

Table 13: Severity levels of the RASLog messages

Severity level	Description
CRITICAL	Critical-level messages indicate that the software has detected serious problems that cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
ERROR	Error-level messages represent an error condition that does not affect overall system functionality significantly. For example, error-level messages may indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
WARNING	Warning-level messages highlight a current operating condition that must be checked or it may lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
INFO	Info-level messages report the current non-error status of the system components; for example, detecting online and offline status of an interface.

For more information on RASLog messages, refer the *Extreme SLX-OS Message Reference*.

AuditLog

DCMCFG audits all the configuration changes in DB. FIRMWARE audit the events occurring during firmware download process. SECURITY audit any user-initiated security event for all management interfaces. Audit log messages are saved in the persistent storage. The storage has a limit of 1024 entries and will wrap around if the number of messages exceed the limit.

The SLX device can be configured to stream Audit messages to the specified syslog servers. Audit log messages are not forwarded to SNMP management stations.

Following are few sample outputs.

```
device(config)# sflow polling-interval 25
2016/06/02-08:48:39, [SFLO-1004], 1067, M1 | Active | DCE, INFO,
MMVM, Global sFlow polling interval is changed to 25.
2016/06/02-08:48:39, [SFLO-1006], 1068, M1 | Active | DCE, INFO,
MMVM, sFlow polling interval on port Ethernet 1/14 is changed to
25.
device# show logging auditlog reverse count 2
394 AUDIT,2016/06/02-08:48:39 (GMT), [DCM-1006], INFO, DCMCFG,
admin/admin/127.0.0.1/console/cli,, SLX9850-4, Event: database
commit transaction, Status: Succeeded, User command: "configure
config sflow polling-interval 25".
393 AUDIT,2016/06/02-08:40:57 (GMT), [SEC-3022], INFO, SECURITY,
```

```
root/root/172.22.224.196/telnet/CLI,, MMVM, Event: logout, Status:
success, Info: Successful logout by user [root].
```

For more information on AuditLog messages, refer to the *Extreme SLX-OS Message Reference* .

When logging off a SSH session that uses <RSA 4096>, the audit log entry will display 127.0.0.1 (localhost) instead of the IP address of the device used to login.

Syslog

RASLog and AuditLog infrastructure makes use of Syslog service running on the SLX device to log messages into the local file system or to remote syslog server. All external RASLog messages and all Audit logs are sent to syslog server. SLX-OS uses **`syslog-ng`** which is an open source implementation of the syslog protocol for Unix and Unix-like systems. It runs over any of the following:

- UDP (default port 514)
- TLS (default port 6514)

A maximum of 4 syslog servers can be configured on any SLX device. These servers can have IPV4 or IPV6 address and reside in mgmt-vrf, default-vrf or user defined VRF. The **`logging syslog-server`** command enables the syslog event capturing on the syslog server. The IP address and VRF-name are configurable parameters.

Following are sample syslog events captured at the syslog server.

```
Jun 2 09:17:42 MMVM raslogd: [log@1588
value="AUDIT"][timestamp@1588 value="2016-06-
02T09:17:42.428106"][tz@1588 value="GMT"][msgid@1588 value="DCM-
1006"][severity@1588 value="INFO"][class@1588
value="DCMCFG"][user@1588 value="admin"][role@1588
value="admin"][ip@1588 value="127.0.0.1"][interface@1588
value="console"][application@1588 value="cli"][swname@1588
value="SLX9540"][arg0@1588 value="database commit transaction"
desc="Event Name"][arg1@1588 value="Succeeded" desc="Command
status"][arg2@1588 value=""configure config snmp-server location
"EMIS Rack 11-1""" desc="ConfD hpath string"] BOMEvent: database
commit transaction, Status: Succeeded, User command: "configure
config snmp-server location "EMIS Rack 11-1"".
Jun 2 09:17:42 MMVM raslogd: [log@1588
value="RASLOG"][timestamp@1588 value="2016-06-
02T09:17:42.420216"][msgid@1588 value="SNMP-1005"][seqnum@1588
value="1071"][attr@1588 value=" M1 | Active | WWN
10:00:00:27:fffffff8:fffff[severity@1588
value="INFO"][swname@1588 value="MMVM"][arg0@1588
value="sysLocation" desc="Changed attribute"][arg1@1588
value="has changed from [End User Premise.] to [EMIS Rack 11-1]"
desc="String Value"] BOMSNMP configuration attribute,
sysLocation, has changed from [End User Premise.] to [EMIS Rack 11-1].
```

For more information on Syslog messages, refer to the *Extreme SLX-OS Message Reference Guide*.

.

Importing a syslog CA certificate

The following procedure imports the syslog CA certificate from the remote host to the device.

1. Connect to the device and log in using an account with admin role permissions.
2. In privileged EXEC mode, enter the **crypto import syslogca** command. Include the full path to the certificate on the host, specify SCP as the protocol, and include the IP address of the host.

```
SLX# crypto import syslogca directory file protocol use-vrf mgmt.-vrf host 10.23.54.56
user jane password: ****
```

Viewing the syslog CA certificate

The following procedure allows you to view the syslog CA certificate that has been imported on the device.

1. Connect to the device and log in using an account with admin role permissions.
2. In privileged EXEC mode, enter the **show crypto ca certificate** command.

This example displays the syslog CA certificates.

```
SLX# show crypto ca certificate
```

Verifying syslog CA certificates

To test whether a syslog CA certificate has been imported on the device, in privileged EXEC mode, enter the **no crypto import syslogca** command and examine the message returned by the system. The command returns an error if there is no syslog CA certificate on the device. If a syslog CA certificate exists on the device, you are prompted to delete it. Enter the no certutil syslogcacert command to retain the certificate.

Example for when no syslog CA certificate is present

```
SLX# no crypto import syslogca
% Error: syslog CA certificate does not exist.
```

Example for when a syslog CA certificate exists on the device

```
SLX# no crypto import syslogca
Do you want to delete syslog CA certificate? [y/n]:n
```

Deleting a syslog CA certificate

The following procedure deletes the syslog CA certificates of all attached Active Directory servers from the device.

1. Connect to the device and log in using an account with admin role permissions.
2. In privileged EXEC mode, enter the **no crypto import syslogca** command. You will be prompted to confirm that you want to delete the syslog CA certificates.

This example deletes the syslog CA certificates.

```
SLX# no crypto import syslogca
Do you want to delete syslogca certificate? [y/n]:y
Warning: All the syslog CA certificates are deleted.
```

LOGS over RELP

Reliable Event Logging Protocol (RELP) is a protocol for reliable delivery of event messages to remote logging servers. This protocol is used in environments which cannot afford to tolerate loss of event messages during transit.

RELP uses TCP for event message transmission. Using TCP provides basic protection for message loss. However, it does not guarantee message delivery under all circumstances. TCP cannot reliably detect that the last message sent has actually reached the destination. However, RELP uses a different method to convey information back to the sender about the messages processed by the receiver. This ensures that the both the sender and receiver always know which messages have been transmitted and which have been received at all points of time, even in case of a connection loss.

Sending logs Over RELP

Use the CLI `logging utility enable relp` to switch between using `syslog` or `rsyslog` over RELP. `syslog` is the default event message transmission protocol for SLX-OS.

1. Navigate to the *Global Configuration* mode.

   ```
   SLX # config terminal
   SLX (config)#
   ```

2. Enable or disable logging over RELP.

   - Enable logging over RELP.

     ```
     SLX (config)# logging utility enable relp
     SLX (config)#
     ```

     When logging over RELP is enabled, logging over SYSLOG is automatically disabled and all event messages are transmitted over RELP.

   - Disable logging over RELP.

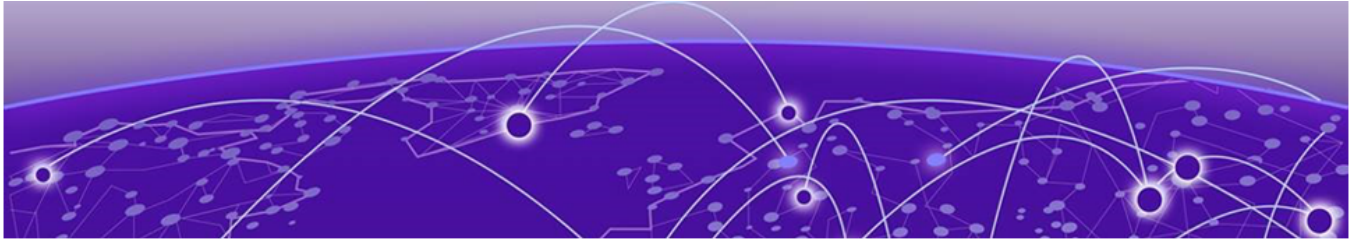
     ```
     SLX (config)# no logging utility enable
     SLX (config)#
     ```

     When logging over RELP is disabled, logging over SYSLOG is automatically enabled and all event messages are transmitted using SYSLOG.

   - When *rsyslog* over is RELP is configured as secured with TLS, the certificates that are used for securing SYSLOG are used by *rsyslog* over RELP.
   - After turning on logging over RELP, and when you use the login credentials of the *SYSLOG* server, then the same credentials are used for logging over RELP.
   - RELP mode does not support *syslog-server host* configuration. This configuration is automatically blocked in the RELP mode. An error message is displayed.

The following example shows the complete configuration for selecting the events to be logged and then enabling logging over RELP.

```
SLX# show run logg
logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
logging utility enable relp
SLX#
```



sFlow

sFlow overview on page 115
sFlow Datagram Flow on page 117
Configure sFlow forwarding on MPLS interfaces on page 118
Feature support matrix for sFlow on page 118
Configuring sFlow on page 119

sFlow overview

The sFlow standard consists of an sFlow agent that resides anywhere within the path of the packet and an sFlow collector that resides on a central server. This release is compliant with sFlow Version 5.

The sFlow agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector at regular intervals. The datagrams consist of information on, but not limited to, packet header, ingress interfaces, sampling parameters, and interface counters. Packet sampling is typically performed by the ASIC. The sFlow collector analyzes the sFlow datagrams received from different devices and produces a network-wide view of traffic flows. You can configure up to five collectors, using both IPv4 and IPv6 addresses.

The sFlow datagram provides information about the sFlow version, its originating agent's IP address, a sequence number, one or more flow samples or counter samples or both, and protocol information.

The sFlow agent uses two forms of operation:

- Time-based sampling of interface counters
- Statistical sampling of switched packets

sFlow can be port based or ACL based.

In port based sFlow, the sampling entity performs sampling on all flows originating from or destined to a specific port. Each packet is considered only once for sampling, irrespective of the number of ports it is forwarded to. Port based sFlow uses the port level sampling rate, if it is configured. Otherwise, it uses the global sampling rate. When port level sampling rate is unconfigured with 'no' option, it will revert back to using the global sampling rate.

Access-list (ACL) based sFlow ensures that sampling is done per flow instead of per port. ACL based sFlow uses global sampling rate .

The following applications does flow based sFLow.

- User ACL based sflow
- VxLAN visibility sflow

Note
When User ACL based sFlow is enabled along with port based sFlow, two samples are generated, one for port based and the other one for User ACL based sFlow. The difference between these two samples are not visible on the collector. However, the difference is visible in the **`show sflow all`** command output (sflow interface/ACL/ VxLan Visibility statistics).

Port-based and flow-based sFlow are supported on physical ethernet ports only.

Note
sFlow counter samples will be generated for all the sflow enabled interfaces even if the interface is down.

Note
On SLX 9740, Port based sFlow is supported on port-channel interfaces and their member ports.

On all devices, except SLX 9740, Port based sFlow is not supported on port-channel interfaces. However, you can configure sFlow on the individual member ports of the port-channel and VE interfaces.

BGP AS-Path

The sFlow packet processing support for the sflow BGP AS path forwarding works when the BGP is up and it advertises routes. sFlow samples with destination IP (DIP) address and source IP (SIP) address that match the route in BGP routing table, collected and sent to the collector are appended with the BGP AS-path information also known as the extended gateway header. In case of samples with DIPs and SIPs that do not have route in BGP routing table and sent to sFlow Collector are not appended with AS-path. However, this does not impact the sFlow operation. This attribute identifies autonomous systems (ASs) through which update message has passed. The last AS traversed by prefix is placed at the beginning of list. You can configure a maximum number of 300 ASs.

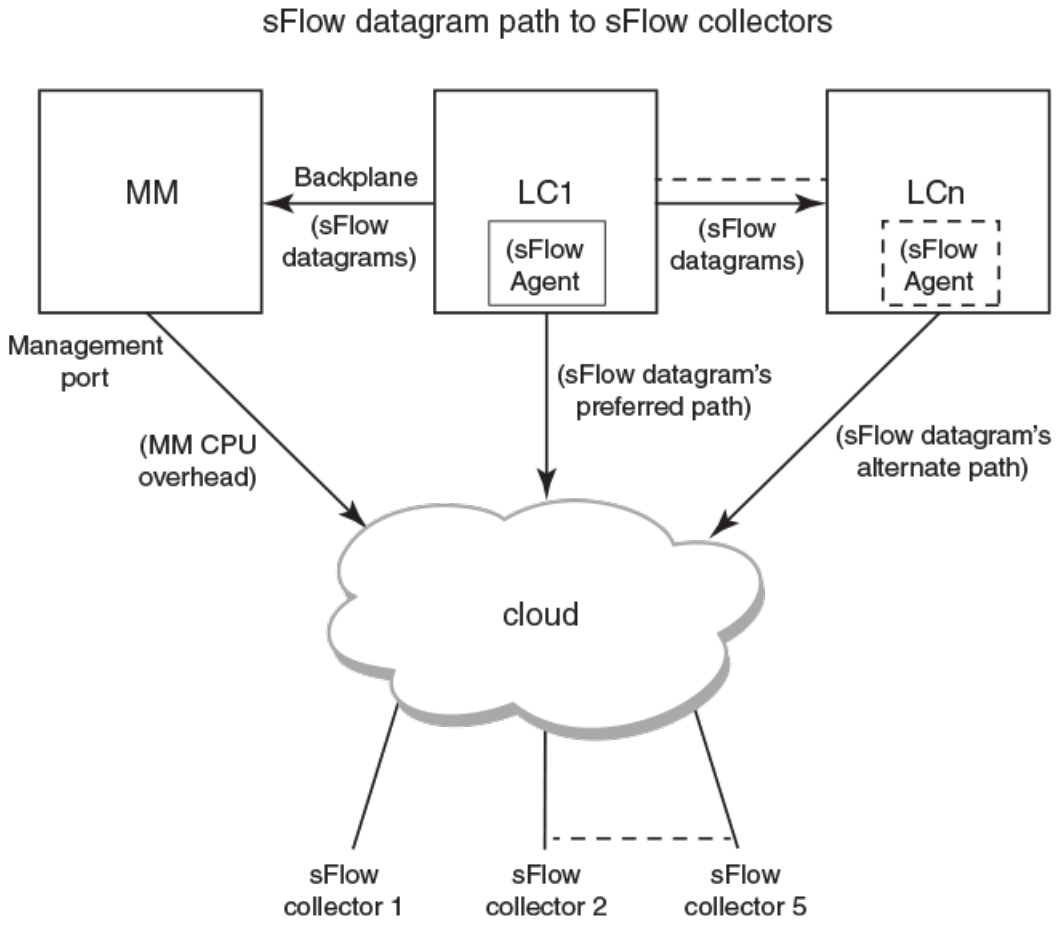
Note
- By default, the BGP AS-path is enabled. It does not requires any specific configuration.
- After enbaling sFlow configuring sample collector, you must disable counter sampling globally or per interface.

BGP Community

A BGP community is used for traffic engineering and dynamic routing policies. It can be added to the route and advertised to all neighbors. The community attribute values are

encoded with an Autonomous System (AS) number in the first two octets, with the remaining two octets defined by the AS. A prefix can have more than one community attribute. A BGP speaker that sees multiple community attributes in a prefix can act based on one, some or all the attributes. A router has the option to add or modify a community attribute before the router passes the attribute on to other peers. In sFlow, based on the standard, the community routing policies can be predicted for prefixes belonging to same community. An AS-path exists in an sFlow sample where a DIP matches the BGP route table but presence of community attribute is optional.

sFlow Datagram Flow



As shown in the diagram above, the sFlow datagram generated on LC1 can be sent to sFlow collector(s) via:

- **LC's own data (in-band) ports** - This has the least CPU overhead in terms of forwarding the sFlow datagram to the collectors.
- **Another LC's data (in-band) ports** - This has some amount of overhead in forwarding the sFlow datagram to the collectors since it has to forward from one LC to another LC before exiting through the other LC's data (in-band) port.

- **MM management port** - This has the maximum CPU overhead since the MM CPU has to process the messages (sflow datagrams) forwarded by the LC and then route them out through its management port.

Note
Wherever possible, you must configure the sFlow collectors in such a way that the sFlow datagram gets routed through the same LC data (in-band) ports as described in option 1 above. If this is not possible, option 2 mentioned above may be considered as the next option. Option 3 is the least preferred in deployed systems due to the maximum CPU overhead.

Configure sFlow forwarding on MPLS interfaces

MPLS interface can be physical or logical. However, sflow can be enabled only on the underlying physical port if the MPLS interface is logical. Hence, the sflow configuration on MPLS interfaces is the same as the physical interface configuration mentioned above.

Feature support matrix for sFlow

The following table captures the sFlowfeature support matrix for this release.

Table 14: sFlow feature support

sFlow Feature	Support
sFlow v5	Supported
sFlow MIB	Supported When the Data source related Table (sFlowFsTable) is retrieved, corresponding sFlowFsReceiver object will continue to return the first entry in the Collector table (sFlowRcvrTable).
ACL-based sFlow	Supported Port-based and flow-based sFlow are supported on physical ethernet ports only.
sFlow support for 802.1x authentication	Supported sFlow .1x authentication support involves providing Extended User name header in the sFlow datagram.
sFlow Sampling for Null0 Interface	Supported (always enabled)
Extended Gateway, Extended router, and NAT/MPLS/URL header formats	No Support for Extended Gateway. Only Raw header and Extended Switch header is supported.
sFlow data source interface	Supported, but does not support front port trunks.
sFlow scanning for inbound, outbound, or both directions on a port	Inbound only

Table 14: sFlow feature support (continued)

sFlow Feature	Support
Multiple collector configuration	A maximum of five IPv4 or IPv6 collectors could be configured and can be part of any of the configured VRFs.
Subagent-ID	Slot number of the interface
Agent IP address	It can be configured through CLI. By default, active MM is used as the Agent IP address.
sFlow source IP and Port	Supports configuration of source IP interface. Source IP port is not configurable.
Maximum sFlow raw packet header size	For IPV6 sFlow sample, the raw packet header size is 256 bytes. For the rest, it is 128 bytes.
sFlow datagram max size	1400 bytes
sFlow counter polling support on per-port, per-VLAN, or per-trunk or per tunnel basis	Supports per-port counter polling only.
Ability to disable sFlow counter polling	Supports global and per-interface level.
All standard if_counters and Ethernet counters	Supported
AS path cleanup timer (v4: BGP communities, v5: BGP next hop router)	Not supported
sFlow support on VxLAN tunnels	Supported In addition to the VxLAN tunnel related information specified in the sFlow Data source flag and Input interface index fields, VxLAN extension headers are supported for Ingress packet sampled before encapsulation and Ingress packet sampled before decapsulation.
sFlow sampling over GRE tunnel	sFlow sampling feature is not supported over GRE tunnel on SLX 9740 and Extreme 8820 devices due to TCAM space restriction.

Configuring sFlow

- Enable sFlow feature globally on the device.
- Configure sFlow collectors and optionally associated UDP ports.
- Configure ACL based sFlow or Enable sFlow forwarding on Physical interfaces.
- Configure other optional sFlow configuration parameters.
- For the SLX 9740 and Extreme 8820 devices, the configurable sample rate value is 1-16000000. For all other devices, the configurable sample rate value is 1-100000.

Configuring sFlow globally

1. Enter the configure terminal command to change to global configuration mode.

```
device# configure terminal
```

2. Enable the sFlow protocol globally.

```
device (config)# sflow enable
```

3. Configure sFlow collectors and optionally associated UDP ports.

```
device(config)# sflow collector 172.22.12.83 6343 use-vrf mgmt-vrf
device(config)# sflow collector fdd1:a123:b123:c123:34:1:1:2 4713 use-vrf vrf2
device(config)# sflow collector fdd1:a123:b123:c123:112:1:1:2 5566 use-vrf default-vrf
```

4. Set the sFlow polling interval (in seconds).

```
device(config)# sflow polling-interval 35
```

5. Set the sFlow sample-rate.

```
device(config)# sflow sample-rate 4096
```

6. Return to privileged EXEC mode.

```
device(config)# end
```

7. Confirm the sFlow configuration status by using the show sflow or show sflow all commands.

```
device# show sflow
```

8. Clear any existing sFlow statistics to ensure accurate readings.

```
device# clear sflow statistics
```



Note
No specific configuration is required for MPLS other than enabling sflow on physical interfaces.

Enabling flow-based sFlow

Perform the following steps, beginning in global configuration mode.



Note
The "deny ACL" rule is not supported for flow-based sflow. Only the permit action is supported.

1. Create an sFlow profile. Be sure to specify the sampling-rate as a power of 2.

```
device(config)# sflow-profile profile1 sampling-rate 256
```

2. Create a standard MAC ACL.

```
device# mac access-list standard acl1
device(conf-macl-std)# permit any
```

3. Create a class map and attach the ACL to the class map.

```
device(conf-macl-std)# class-map class1
device(config-classmap)# match access-group acl1
```

4. Create a policy map and attach the class map to the policy map.

```
device(config-classmap)# policy-map policy1
device(config-policymap)# class class1
```

5. Use the **map** command to add an sFlow profile name.

   This example assigns the profile name "profile1."

```
device(config-policymap-class)# map sflow profile1
```

6. Switch to interface configuration mode.
7. Bind the policy map to an interface.

Disabling flow-based sFlow on specific interfaces

To disable sFlow on a specific interface, perform the following steps in interface configuration mode.

Note
Disabling sFlow on an interface port does not completely shut down the network communication on the interface port.

1. Disable the sFlow interface.

```
device(conf-if)# no sflow enable
```

2. Return to privileged EXEC mode.

```
device(conf-if)# end
```

3. Switch to interface configuration mode.

```
device(config-policymap-class)# exit

device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)#
```

4. Disable flow-based sFlow by removing the policy map.

```
device(conf-if-eth-0/1)# no service-policy in
```

5. Confirm the sFlow configuration status on the specific interface.

```
device# show sflow interface ethernet 0/1
```

Configuring sFlow for interfaces

After the global sFlow configuration, sFlow must be explicitly enabled on all the required interface ports.

Note
On SLX 9740, Port based sFlow is supported on port-channel interfaces and their member ports.

On all devices, except SLX 9740, Port based sFlow is not supported on port-channel interfaces. However, you can configure sFlow on the individual member ports of the port-channel and VE interfaces.

Note
When sFlow is enabled on an interface port, it inherits the sampling rate and polling interval from the global sFlow configuration.

Enabling and customizing sFlow on specific interfaces

Perform the following steps in privileged EXEC mode to enable and customize sFlow on an interface. This task assumes that sFlow has already been enabled at the global level.

In general, packets are typically sampled according to the configured rate. To prevent synchronization with any periodic patterns in the traffic, the sampling process has a random element to it. With higher sampling numbers, the actual sampled packet rate is approximately equal to the configured rate.

1. Enter the **interface** command.
2. Use the **sflow enable** command to enable sFlow on the interface.
3. Configure the sFlow polling interval.
4. Set the sFlow sample-rate.
5. (Optional) Confirm the sFlow configuration status on the specified interface using the **show sFlow interface** command.

   Following is a sample output of the **show sFlow interface** command.

```
device# show sflow interface tenGigabitEtherent 1/0/24

sFlow info for interface TenGigabitEthernet 1/0/24
-------------------------------------------------
Port based sflow services are:         disabled
Flow based sflow services are:         enabled
Configured sampling rate:              0 pkts
Actual sampling rate:                  0 pkts
Counter polling interval:              0 secs
Samples received from hardware:        61
Port backoffThreshold :                0
Counter samples collected :            0

device#
```

Configuring an sFlow policy map and binding it to an interface

Perform the following steps to configure an sFlow policy map and bind it to an interface.

1. Enter the **configure terminal** command to change to global configuration mode.

```
switch# configure terminal
```

2. Create a standard MAC access control list (ACL).

```
switch# mac access-list standard acl1
switch(conf-macl-std)# permit any
```

3. Create a class map and attach the ACL to the class map.

```
switch(conf-macl-std)# class-map class1
switch(config-classmap)# match access-group acl1
```

4. Create a policy map and attach the class map to the policy map.

```
switch(config-classmap)# policy-map policy1
switch(config-policymap)# class class1
```

5. Add an sFlow profile name by using the command.

   This example assigns the profile name ""

6. Bind the policy map to an interface.

Disabling sFlow on specific interfaces

Note
Disabling sFlow on the interface port does not completely shut down the network communication on the interface port.

To disable sFlow on a specific interface, perform the following steps in interface configuration mode.

1. Disable the sFlow interface.
2. Return to privileged EXEC mode.
3. Confirm the sFlow configuration status on the specific interface.

sFlow agent address

An sFlow agent address provides the SNMP connectivity to the agent in accordance with the sFlowAgentAddress definition in the sFlow RFC. You can configure the sFlow agent address similar to the source IP configuration instead of using the default agent address, which is set to the IPv4 address of the management port of the active management module. Use the **sflow agent- address** command to configure the sFlow agent IPv4 or IPv6 address.

Configuring sFlow agent address

Use the following steps to configure the sFlow agent address.

Note
If the sFlow agent address is not configured, or if sFlow agent address configuration is removed or when the IP address of a specified interface corresponding to the specified agent-address IP address type is not configured, the IPv4 address of the management port of the active management module will be used.

From the global configuration mode, use the **sflow agent-address** to configure the sFlow agent address.

```
device# configure terminal
(device-config)# sflow agent-address ipv4 ethernet 2/5
```

Use the **no sflow agent-addres** command to removed the sFlow agent address configuration.

```
(device-config)# no sflow agent-address
```

Limitations and restrictions

The sFlow agent address feature has the following limitations.

- The **show sflow** command displays the IP address of the selected interface for agent-address field. It does not display the specified interface for agent-address field. Use the **show running-config** command to display the agent address interface information.

Configuring Update Destination MAC in sFlow Streams for Routed Packets

Enable sFlow globally before configuring this setting. For more information, see Configuring sFlow globally on page 120.

1. Enter the configure terminal command to change to global configuration mode.

```
device# configure terminal
```

2. Enable *Update Destination MAC in sFlow Streams*.

```
device (config)# sflow update-destination-mac
```

3. Confirm the sFlow configuration status by using the **show sflow** or **show sflow** all commands. You can also use the **show running-config** command.

```
device# show sflow
```

4. Clear any existing sFlow statistics to ensure accurate readings.

```
device# clear sflow statistics
```



Note
No specific configuration is required for MPLS other than enabling sflow on physical interfaces.

Configuration example

Global configuration

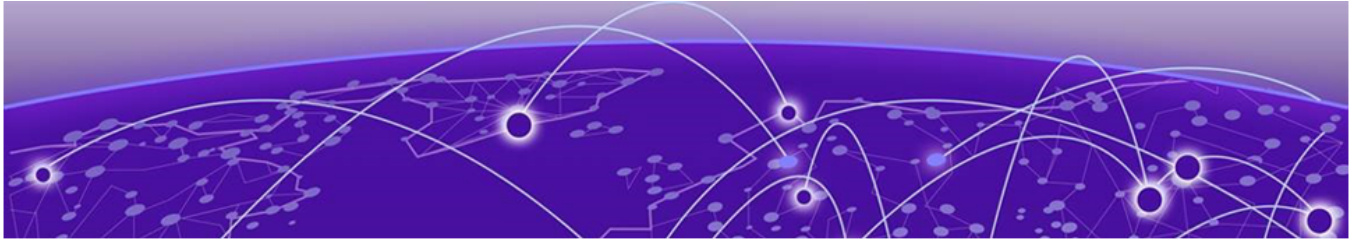
```
device(config)# sflow enable
2024/01/23-10:03:34, [SFLO-1001], 4337, DCE, INFO, switch, sFlow is enabled globally.
device(config)# no sflow enable
2024/01/23-10:03:53, [SFLO-1001], 4338, DCE, INFO, switch, sFlow is disabled globally.
device(config)# sflow sample-rate 4096
2024/01/23-10:04:15, [SFLO-1003], 4339, DCE, INFO, switch, Global sFlow sampling rate is
changed to 4096.
device(config)# no sflow sample-rate
2024/01/23-10:04:45, [SFLO-1003], 4340, DCE, INFO, switch, Global sFlow sampling rate is
changed to 2048.
device(config)# sflow polling-interval 30
2024/01/23-10:05:01, [SFLO-1004], 4341, DCE, INFO, switch, Global sFlow polling interval
is changed to 30.
device(config)# no sflow polling-interval
2024/01/23-10:05:19, [SFLO-1004], 4342, DCE, INFO, switch, Global sFlow polling interval
is changed to 20.
device(config)# sflow collector 172.22.108.57 6343
2024/01/23-10:06:00, [SFLO-1007], 4343, DCE, INFO, switch, 172.22.108.57 is configured as
sFlow collector.
device(config)# sflow collector 10.1.15.2 6343 use-vrf default-vrf
2024/01/23-10:06:47, [SFLO-1007], 4344, DCE, INFO, switch, 10.1.15.2 is configured as
sFlow collector.
device(config)# vrf red_vrf
device(config-vrf-red_vrf)# address-family ipv4 unicast
device(vrf-red_vrf-ipv4-unicast)# exit
device(config-vrf-red_vrf)# exit
device(config)# sflow collector 100.1.1.2 6343 use-vrf red_vrf
2024/01/23-10:08:42, [SFLO-1007], 4345, DCE, INFO, switch, 100.1.1.2 is configured as
sFlow collector.
device(config)# sflow update-destination-mac
2024/01/23-10:09:26 , [SFLO-1021], 39217, DCE, INFO, DUT-3, Updating of destination MAC
in sFlow samples for routed packets is enabled globally.
device(config)# do show sflow
```

```
 show sflow
sFlow services are: enabled
sFlow null0 sampling: enabled
Global default sampling rate: 2048 pkts
Global default counter polling interval: 20 secs
sFlow Agent-ID address: 10.24.6.102
sFlow update-destination-mac: enabled
Collector server address       Vrf-Name           Sflow datagrams sent
-------------------------------------------------------------------------------
10.1.15.2:6343                 default-vrf            0
100.1.1.2:6343                 red_vrf                0
172.22.108.57:6343             mgmt-vrf               0

ACL based samples collected (permit): 0
ACL based samples collected (deny): 0
VxLAN Visibility samples collected: 0
VxLAN Gateway samples collected: 0

device(config)# do show run sflow
sflow enable
sflow update-destination-mac
sflow collector 10.1.15.2 6343 use-vrf default-vrf
sflow collector 100.1.1.2 6343 use-vrf red_vrf
sflow collector 172.22.108.57 6343 use-vrf mgmt-vrf

device(config)# no sflow collector 172.22.108.57
2024/01/23-10:12:38, [SFLO-1007], 4347, DCE, INFO, switch, 172.22.108.57 is unconfigured
as sFlow collector.
device(config)# no sflow collector 10.1.15.2 6343 use-vrf default-vrf
2024/01/23-10:13:13, [SFLO-1007], 4348, DCE, INFO, switch, 10.1.15.2 is unconfigured as
sFlow collector.
device(config)# no sflow collector 100.1.1.2 6343 use-vrf red_vrf
2024/01/23-10:13:54, [SFLO-1008], 4349, DCE, INFO, switch, All the sFlow collectors are
unconfigured.
device(config)# no sflow update-destination-mac
2023/01/23-10:14:10, [SFLO-1022], 39216, DCE, INFO, DUT-3, Updating of destination MAC in
sFlow samples for routed packets is disabled globally.
```

Interface configuration

```
device(conf-if-eth-1/14)# sflow en

2015/12/02-02:49:13, [SFLO-1002], 73, M1 | Active | DCE, INFO, Device, sFlow is
enabled for port Ethernet 1/14.

device(conf-if-eth-1/14)# no sflow enable
2015/12/02-03:28:09, [SFLO-1002], 90, M1 | Active | DCE, INFO, Device, sFlow is
disabled for port Ethernet 1/14.


device(conf-if-eth-1/14)# sflow sample-rate 8192

2015/12/02-03:13:26, [SFLO-1005], 86, M1 | Active | DCE, INFO, Device, sFlow sampling
rate on port
Ethernet 1/14 is changed to 8192.

device(conf-if-eth-1/14)# no sflow sample-rate

2015/12/02-03:26:39, [SFLO-1005], 88, M1 | Active | DCE, INFO, Device, sFlow sampling
rate on port
Ethernet 1/14 is changed to 4096.
```

```
device(conf-if-eth-1/14)# sflow polling-interval 40

2015/12/02-03:13:40, [SFLO-1006], 87, M1 | Active | DCE, INFO, Device, sFlow polling
interval on
port Ethernet 1/14 is changed to 40.

device(conf-if-eth-1/14)# no sflow polling-interval

2015/12/02-03:26:47, [SFLO-1006], 89, M1 | Active | DCE, INFO, Device, sFlow polling
interval on port Ethernet 1/14 is changed to 30
```



Threshold Monitoring

Threshold Monitoring on page 127
Configuring Message Rate Limiting Constraints for Threshold Monitoring on page 128
Configuring Threshold Monitor on page 129
MAC Collision Detection and Alarm on page 130

Threshold Monitoring

A device's good health status and the adequate performance of various resources used by it ensures that the device is working as intended and is continuously available for performing its task.

Monitoring the available resources and generating traps and alerts when pre-set user configured thresholds are breached, is the fastest way to react to changes in the monitored device's health and performance.

SLX-OS enables monitoring of system and Layer 2, Layer 3, and ACL hardware resources. Thresholds can be set for each parameter being monitored. Both high threshold and low threshold values can be configured for each parameter.

Actions

When a threshold is breached, that is, when the monitored parameter crosses the configured high threshold value, or, when the parameter falls below the lower threshold, you can take one of the multiple actions that are available for use.

The following actions are available:

- RASLOG - A RASLOG entry is generated
- SNMP - A SNMP trap is generated
- all - Both RASLOG entry is created and SNMP trap is generated
- none - no action is taken
- loginfo - This option is only available when monitoring hardware resources such as CPU and memory. When selected, additional information is also gathered till further action is taken.

These actions ensure that an anomalous event is recorded in one form or another, and then, can be used later to troubleshoot or for RCA of the issue.

Rate Limiting

Since it is possible that multiple entries/traps can be generated for an event, options are available to rate limit the generation of these events/traps. Before SLX-OS 20.5.3, rate limiting was configurable on a per monitored parameter basis. However, from SLX-OS 20.5.3 onwards, rate limiting is configured globally and is applicable to all monitored parameters.

Rate limiting consists of two configurable constraints:

- the number of messages (X)
- the duration (Y) (in seconds)

When configured, the constraints can be summed as: *Generate a maximum of X messages in Y units of time*. Messages can be RASLOG or SNMP or Both and this depends on the *action* configured for that specific monitored parameter.

Monitored Parameters

The following hardware parameters are monitored:

- CPU
- Memory

The following parameters are also monitored:

- BFD Sessions
- ECMP
- Hosts
- LIF
- MAC Table
- Next Hop
- Route
- SFP
- VxLAN Tunnels
- ACL Hardware Resources

Configuring Message Rate Limiting Constraints for Threshold Monitoring

An event can cause multiple messages of different types to be generated simultaneously.

Since it is possible that multiple entries/traps can be generated for an event, options are available to rate limit the generation of these events/traps. Without rate limiting, there is a possibility that the message handling subsystem of the device getting overwhelmed while handling these messages and causing the device to crash.

Rate limiting consists of two configurable constraints:

- the number of messages (X)
- the duration (Y) (in seconds)

When configured, the constraints can be summed as: *Generate a maximum of X messages in Y units of time*. Messages can be RASLOG or SNMP or Both and this depends on the *action* configured for that specific monitored parameter.

To configure the rate limiting constraints:

1. Navigate to the Global Configuration Mode.

```
SLX# configure terminal
SLX (config)#
```

2. Set the *count* parameter.

```
SLX (config)# threshold-monitor hardware-resources count 10
SLX (config)#
```

   The *count* controls the maximum number of events to be generated in the configured time interval. A maximum number of sixty (60) events can be generated for each time interval. The default is four (4).

3. Set the *interval* parameter.

```
SLX (config)# threshold-monitor hardware-resources interval 300
SLX (config)#
```

   The *interval* controls the time duration in seconds. In this example, a maximum of 10 messages can be generated every 300 seconds. The range is 30-900 seconds and the default is 30 seconds.

This example shows the complete configuration for the rate limiting constraints.

```
SLX# configure terminal
SLX (config)# threshold-monitor hardware-resources count 10
SLX (config)# threshold-monitor hardware-resources interval 300
SLX (config)#
```

Configuring Threshold Monitor

Threshold monitoring ensures that usage of resources are monitored constantly and events are triggered whenever an anomaly in usage occurs.

The following hardware parameters are monitored:

- CPU
- Memory

The following parameters are also monitored:

- BFD Sessions
- ECMP
- Hosts
- LIF
- MAC Table
- Next Hop
- Route
- SFP

- VxLAN Tunnels
- ACL Hardware Resources

For each parameter, you can set the *high-threshold* and *low-threshold* value. You can specify the *action* to be taken when one of these thresholds is breached.

1. Navigate to the Global Configuration Mode.

```
SLX# configure terminal
SLX (config)#
```

2. For the parameter to be monitored, set the thresholds. Here we are configuring ECMP thresholds and the action to be taken when a threshold is breached.

```
SLX (config)# threshold-monitor ecmp high-limit 98 low-limit 65 action both
SLX (config)#
```

The above configuration is for the utilization of the ECMP Table. The current values of number of ECMP Next Hop entries (in %) is compared with the configured profile limits and against the available hardware space. An alarm is raised when the number of entries falls below the configured low threshold value of 65% or crosses the configured high threshold of 98%. Both SNMP traps and RASLOG entries are generated for these events.

The following is the above configuration

```
SLX# configure terminal
SLX (config)# threshold-monitor ecmp high-limit 98 low-limit 65 action both
SLX (config)#
```

The following is a configuration example for monitoring the Route table usage.

```
SLX# configure terminal
SLX (config)# threshold-monitor route high-limit 80 low-limit 50 action both
SLX (config)#
```

MAC Collision Detection and Alarm

Note

This feature is only applicable for the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices.

Due to limited resources in the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices, it is possible that the dynamically learned and statically configured MACs may cause the MAC table to get filled up to its maximum number of entries. These devices can support a maximum of 96,000 (Ninety Six Thousand) MAC entries.

Once the MAC table usage goes beyond the user configurable high threshold limit, it might cause entries not to be properly programmed in the MAC table and could lead to flooding. Users are notified on such events happening through log entries.

Similarly, when MAC Collisions happen, users are notified through log entries and stale entries are automatically removed from the MAC Table. For every MAC collision, a RAS Log entry is generated. However, this generation is rate limited to a maximum of 4 notifications every 30 seconds. The last 256 collisions with time-stamp are also stored for debugging purposes.

The following is an example of the RAS Log that is generated for every MAC Collision that occurs.

```
DUT7# 2024/09/20-06:56:57, [HSL-1069], 28029, DCE, ERROR, DUT7,
                        MAC collision occurred in HW for MAC:[0000.0001.376d], VlanId/
BDId:100 (V)
```

The following additional RAS Log entries are generated when the available resources exceed or reach specified levels. This message is generated when the MAC Address Table reaches the configured High Threshold Limit.

```
2024/09/17-10:02:32, [L2SS-1036], 24829, DCE, INFO, DUT7,
                             MAC-address-table reached the high threshold limit of 85
percent
```

This message is generated when the MAC address table reaches 100% of its guaranteed limit.

```
2024/09/17-10:02:38, [L2SS-1031], 24830, DCE, INFO, DUT7,
                        MAC-address-table has reached 100 percent full.
```