BROCADE

CONFIGURATION GUIDE

Brocade SLX-OS Monitoring Configuration Guide, 17r.1.01a

Supporting the Brocade SLX 9850 and 9540 Devices

53-1005161-02
16 October 2017

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	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. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.

Click the **Support** tab and select **Document Library** to access product documentation on MyBrocade or www.brocade.com. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online or by telephone. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: • Case management through the MyBrocade portal. • Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • Toll-free numbers are available in many countries. • For areas unable to access a toll-free number: +1-408-333-6061

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Document

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for SLX-OS Release 17r.1.01, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- Brocade SLX 9850-4 router
- Brocade SLX 9850-8 router
- Brocade SLX 9540 switch

To obtain information about other Brocade OS versions, refer to the documentation specific to that version.

Interface module capabilities

The following table lists the supported capabilities for the following Brocade SLX 9850 interface modules:

- BR-SLX9850-10Gx72S-M
- BR-SLX9850-100Gx36CQ-M
- BR-SLX9850-10Gx72S-D
- BR-SLX9850-100Gx36CQ-D

TABLE 1 Brocade SLX 9850 interface modules capabilities

Capability	Modular interface module
MPLS	Yes
Packet Buffer memory per interface module	12GB (BR-SLX9850-10Gx72S-M) 36GB (BR-SLX9850-100Gx36CQ-M) 8GB (BR-SLX9850-10Gx72S-D) 24GB (BR-SLX9850-100Gx36CQ-D)

What's new in this document

There are no new feature added since the SLX-OS 17r.1.01 release.

Operation, Administration, and Maintenance (OAM)

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.

Limitation and Restriction

CFM is supported on port channels with all member ports belonging to same line card. However, CFM is not supported on port channels with member ports across line cards.

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

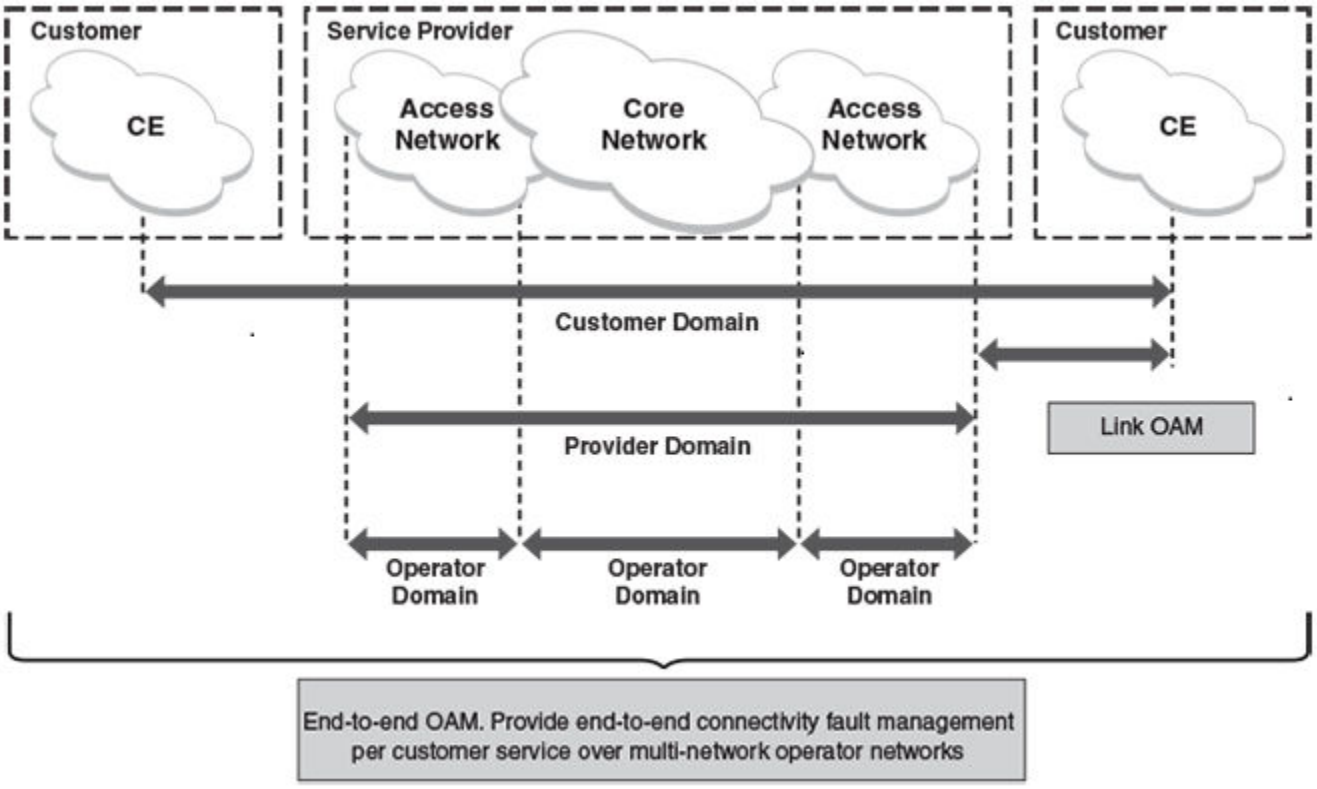
Bridges are increasingly used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM provides capabilities for detecting, verifying and isolating connectivity failures in such networks.

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 1 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 1 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 1 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.

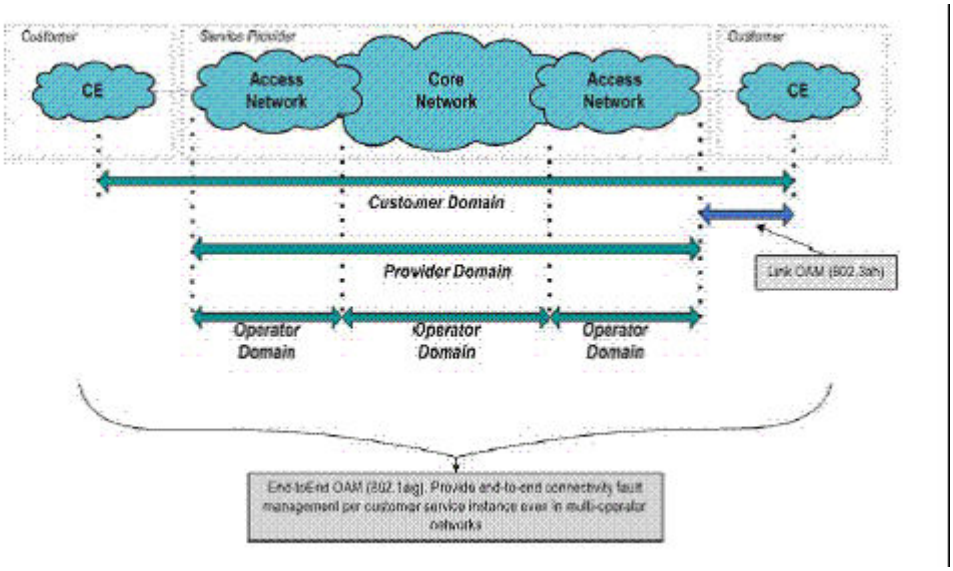
802.1ag Connectivity Fault Management

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 2 OAM Ethernet tools



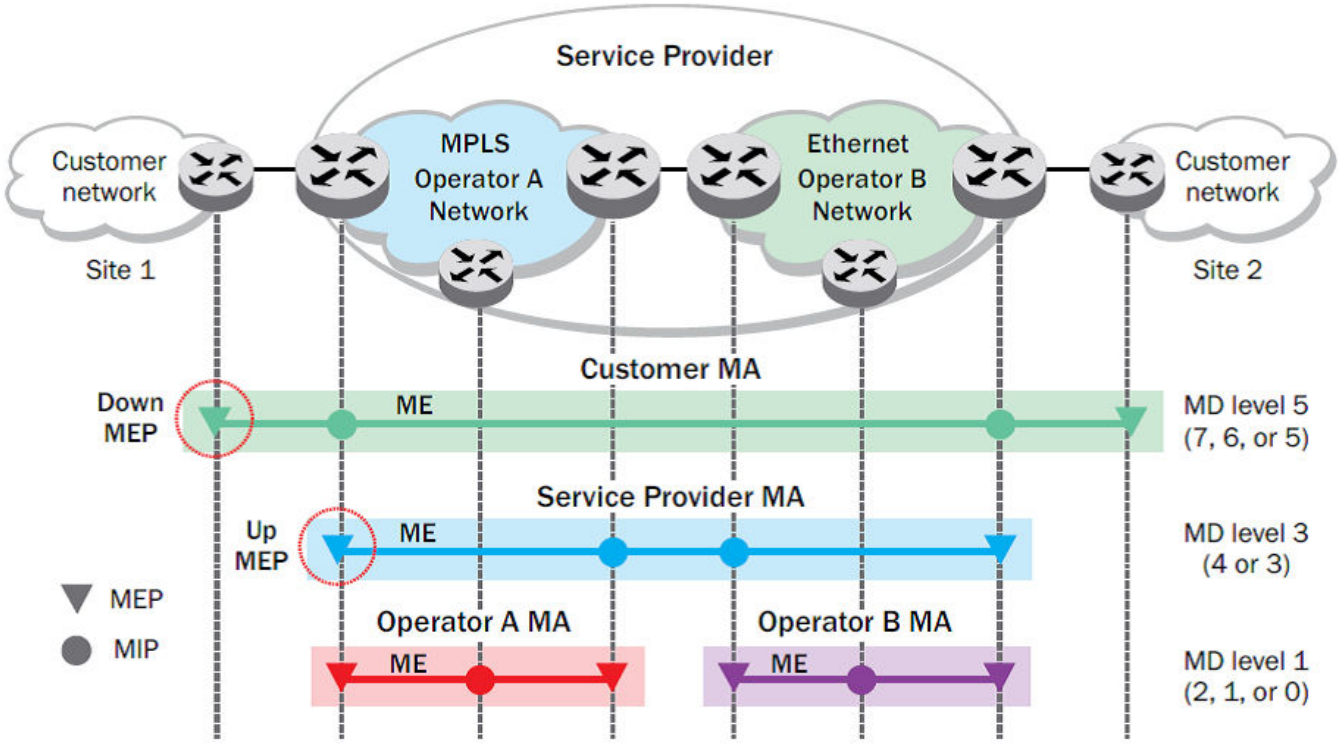
Maintenance Domain (MD)

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 3 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 and name and enters the specific MD mode specified in the command argument.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 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

Perform the following steps to create and configure a Maintenance Association (MA).

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 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 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 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 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)# 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 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

This feature enables CFM Maintenance End Point (MEP) on double tagged VPLS end point.

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
```

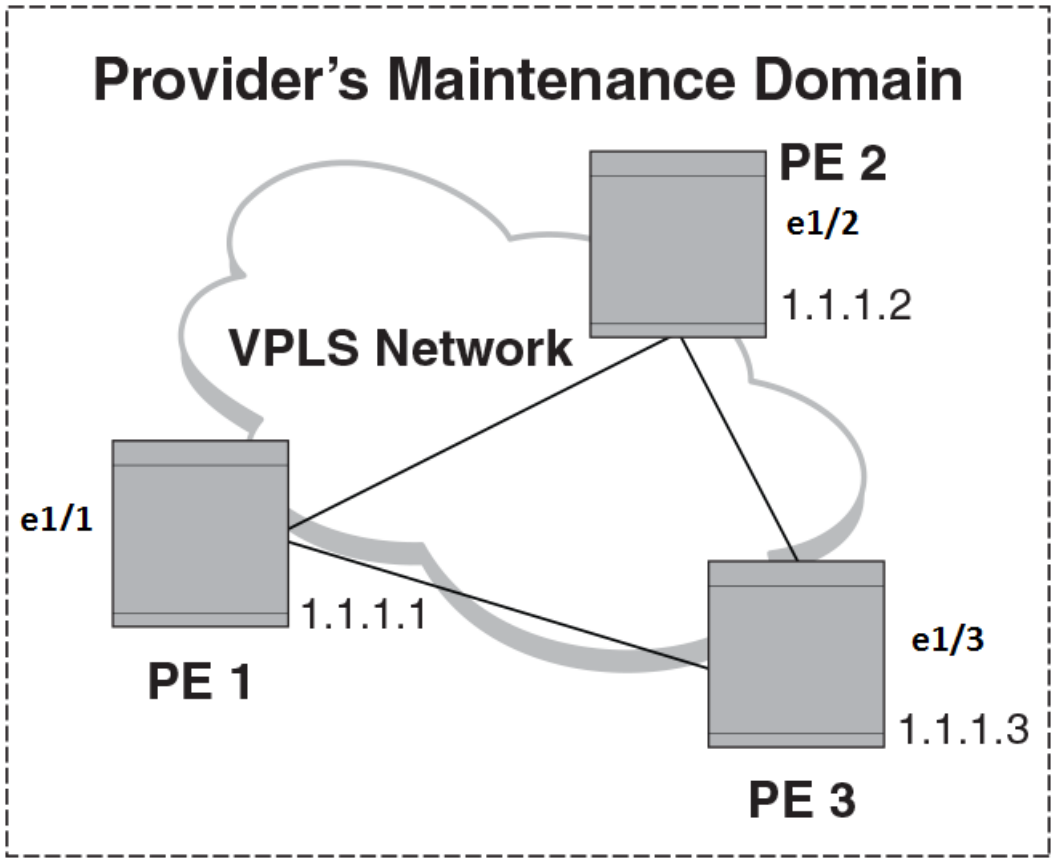
Monitoring the status of devices in a VPLS network in a Provider's Maintenance Domain

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 4 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 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

CFM LBM message is generated when the CFM loopback test is performed. The packet is destined to the MAC address which the loopback test intends to reach. You can verify the connectivity using the **CFM loopback** command.

```
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.
```

Port status TLV

Port status TLV is carried in every CCM message and it carries the state of transmitting port. The state can be either 1 or 2.

- 2 - Port state is Forwarding
- 1 - Port state other than Forwarding

Port status TLV is supported only on VLAN and VPLS.

Configuring port status TLV

Port status TLV is optional and will be carried in a CCM message only if it is enabled in the MEP configuration. Port Status TLV for a specified MEP can be enabled using the following command.

```
device(config-cfm)# domain name md1 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)# tlv-type port-status-tlv
```

The **no** form of the command disables the Port Status TLV for the specified MEP.

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 SLX-OS 17r.1.01.

- 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 support in SLX-OS 17r.1.01a

SLX-OS 17r.1.01a 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 VxLAN, MC-LAG and VLL

Limitations and Restrictions

The existing timestamp on the SLX 9540 device is causing a failure in Y.1731 based on the delay measurement when on one end there is an SLX 9540 device, and on the other end there is an SLX 9540 device, NetIron MLXe or NetIron CER device, or an SLX 9850 device. The same feature is working properly when both end devices are SLX 9850 devices or NetIron MLXe devices.

In addition, SLX-OS 17r.1.01a has the following limitations.

- SNMP MIBs and traps are not supported.
- Maximum value of frame_delay could be 4 seconds. If a frame delay response packet is received after this 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.

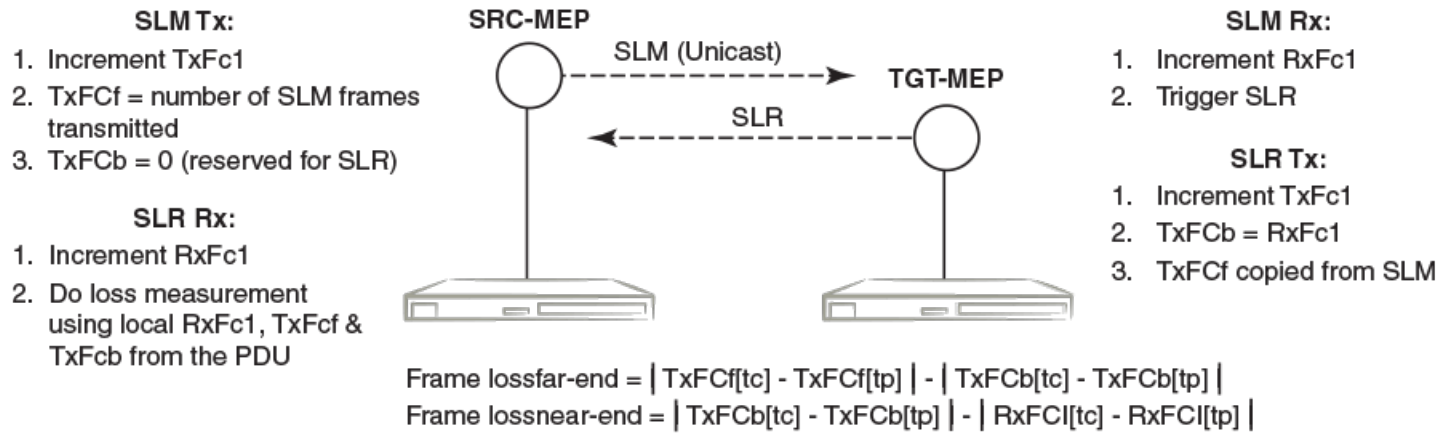
Synthetic loss measurement is a mechanism to measure frame loss using synthetic frames, rather than data traffic. A number of synthetic frames are sent and received, and the number of those that are lost is hence calculated to measure the loss.

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 5 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.

Loss measurement calculation

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

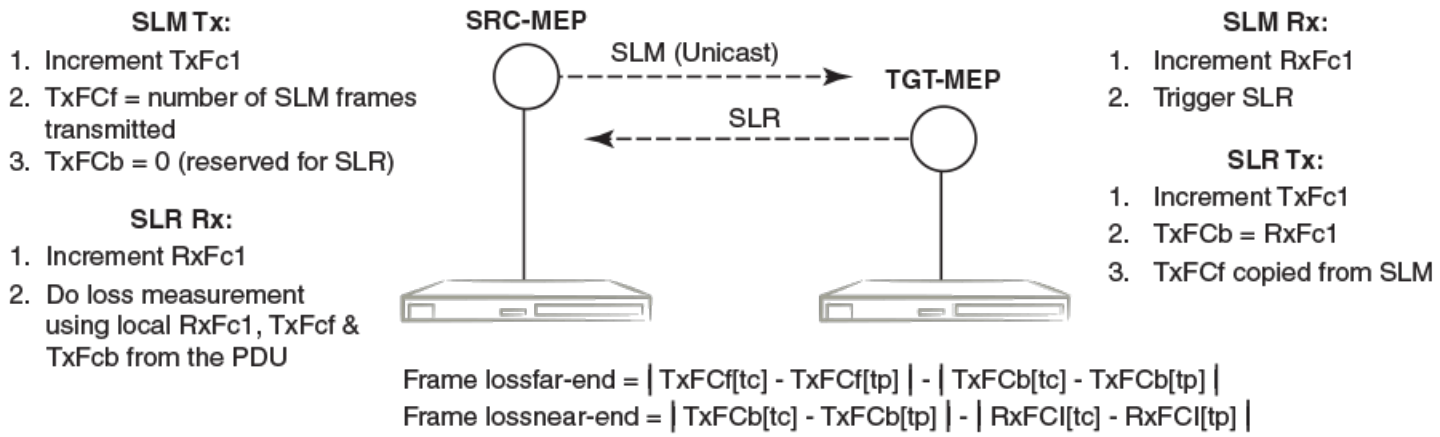
When a valid DMM frame is received by a MEP, a DMR frame is generated and transmitted to the requesting MEP. A DMM frame with a valid domain level and a destination MAC address equal to the receiving MEP's MAC address is considered as a valid DMM frame. There are two additional timestamps which are used 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 6 Two-Way ETH DM



Profiles

Brocade 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 2 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 3 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 ETH-DM or ETH-SLM functionality will not be accurate if VPLS is point to multipoint.
- 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 and action 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.

Interoperability considerations

The Two-way ETH-DM or ETH-SLM on an SLX device can interoperate with Brocade MLX, XMR, CES, and CER if long MAID is configured on them and only with either default CoS or random CoS.

IEEE 802.1ag Long MAID format

Maintenance Association Identifier (MAID) is a 48 byte field included in the Continuity Check Message (CCM) frame to identify the Maintenance Domain (MD) and Maintenance Association (MA) to which this CCM belongs to. This helps in detecting cross connection errors in the service.

IEEE 802.1ag standard defines two possible formats for MAID.

- Short format which does not include MD maintenance domain name and has only short MA name.
- Long format which includes MD name.

By default, short MAID format is configured when a MA is configured. You can set the MAID format for a particular maintenance association to long, using the **maid-format** command.

```
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 30 vlan-id 30 priority 7
device(config-cfm-md-md1)# maid-format long
```

The no form of the command sets the maid format back to short. For more information on commands, please refer the SLX-OS Command Reference guide.

> NOTE
> The maid format cannot be changed after a MEP is configured under that MA. You must delete the MEP and then change the MAID format.

Scalability considerations

- A maximum of 128 test profiles can be created on a system.
- A maximum of 32 action profiles can be created on a system.

- A maximum of 1024 Two-Way ETH-DM or Two-Way ETH-SLM sessions can be configured over 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.
- We recommend that you limit the number of packets sent from the node for measurement to 1280 across maximum of 128 scheduled sessions that can be active at a time across all Y.1731 modules. Any number of packets sent exceeding this limit is not supported by SLX-OS, release 17r.1.01.

Configuring Y.1731 Performance Monitoring

To configure the Y.1731 performance monitoring feature on your Brocade 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 Brocade 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 **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 daily 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 900
```

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 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 1/2
```

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 Brocade 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 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 1/2
```

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

To configure a scheduled measurement session, a test profile must be attached to the MEP-RMEP pair.

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 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 1/2
```

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 following instructions to initiate the on-demand Two-Way ETH-DM or Two-Way ETH-SLM feature.

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
```

Displaying the Two-Way ETH-DM information

Use the following instructions to display 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

Use the following instructions to display 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

Use the following instructions to display Two-Way ETH-SLM information.

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

Use the following instructions to clear 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 (EFM)

The IEEE 802.3ah Ethernet in First Mile (EFM) specifies the protocols and ethernet interfaces for using ethernet access links as a first-mile technology.

Using ethernet in the EFM solution, the user gains broadcast Internet access, in addition to services like Layer 2 transparent LAN services, voice services over ethernet access networks, video, and multicast applications. This 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, namely 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 within 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 utilizing an IP layer.

The functionality of the 802.3ah protocol can be summarized 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 once 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.

Following functionalities are not supported:

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

On SLX-OS device, Link OAM configuration is allowed on VPLS and VLL endpoint(s). Note that the support for VPLS and VLL endpoints is available only when Link OAM is configured on the link between CE (passive) and PE (active).

NOTE
Local loopback is supported only for one port per line card.

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 allows to distinguish OAM PDU frames from other frames.

NOTE
Currently, the support is only for Information and loopback Control OAMPDUs

Network devices are identified along 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 pre-requisite or support for configuration to consider the discovery status as unsatisfied. Hence any capability received from the peer will be deemed as 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 local ethernet interface specified.

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

NOTE
Brocade recommends that when in loopback mode, you should remove the loopback ports from the active network topology to reduce the impact of protocol flaps.

For more information on commands, please refer the Brocade SLX-OS Command Reference supporting the SLX 9850 and 9540 Devices.

Configuring Link OAM

To configure the link OAM, perform the following steps.

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
```

   NOTE
   The support for this configuration is restricted. You cannot configure allow-loopback on more than one port per line card.

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
```

Trace-l2 protocol

Trace-l2 protocol overview

Trace-l2 traces is a proprietary protocol that traces the traffic path to a specified device in a VLAN. Also, it can be used to probe all reachable paths to all devices in a VLAN. It does the following:

- Traces a particular IP, MAC or hostname in a VLAN.
- Probes the entire Layer 2 topology.
- Displays the input or output ports of each hop in the path.
- Displays the round trip travel time of each hop.
- Displays hops in a VLAN that form a loop.
- Displays each hop's Layer 2 protocol such as STP, RSTP, 802.1w, SSTP, metro ring, or route-only.

The resulting trace displays a report that provides information about a packet's path to a device, such as hop and port information and travel time. It also can locate any Layer 2 loop in a VLAN. The probed Layer 2 information is discarded when a new **trace-l2** command is issued again.

For each hop in the path, trace-l2 displays its input/output port, Layer 2 (L2) protocols of the input port, and the microsecond travel time between hop and hop. It also prints out the hops which form a loop, if any. Displaying L2 topology lets a user easily obtain information of all hops.

Following are the benefits provided by the Trace-L2 feature.

- It can be used to check the L2 connectivity between Brocade devices for a particular vlan which supports Trace-L2 feature using IP address, Mac address or DNS hostname of the device.
- It can be used to probe entire L2 topology for a particular vlan to verify the new logical topology after deploying loop resolution protocols such as xSTP.
- It can be used to determine if the L2 topology for a particular vlan has any loops due to the incorrect or failure in protocol convergence for xSTP.

Configuration considerations

The configuration considerations are as follows:

- Trace-l2 is enabled on the Brocade devices. It can be used to trace traffic only to devices.
- The devices that will participate in the trace-l2 protocol must be assigned to a VLAN and all devices on that VLAN must be Brocade devices that support the trace-l2 protocol.
- Brocade devices, as well as other vendor devices, that do not support the trace-l2 protocol, simply forward trace-l2 packets without a reply. Hence, these devices are transparent to the trace-l2 protocol.
- The destination for the packet with the trace-l2 protocol must be a device that supports the trace-l2 protocol and the destination cannot be a client, such as a personal computer, or devices from other vendors.

- Trace-l2 follows the xSTP path if enabled in the system.
- Trace-L2 does not support VPLS.
- Trace-L2 with MCT is not supported.

Tracing a traffic path

The trace-l2 protocol is enabled on a VLAN. You can trace the traffic path of a packet by entering a command such as the following.

```
device(config)#trace-l2 vlan 10 2.2.2.2
```

The *destination* can be a MAC address, an IP address, or a host. You can enter the destination in one of the following formats:

- HHHH.HHHH.HHHH - Destination MAC address
- A.B.C.D - Destination IP address
- ASCII string - destination host name

The command displays the following information.

```
device# trace-l2 vlan 10 2.2.2.2
trace-l2 reply vlan 10 from e1/1/3, 2.2.2.2, total round trip = 988 microsec
  hop input  output IP and/or MAC address       microsec comment
   1   e1/1/3       2.2.2.2 748e.f82b.a800        988    802-1w
```

In the output above, the last hop is the destination. Because 10.1.1.2 and 10.2.2.2 are addresses of the same device, the device can use 10.1.1.2 in the reply.

In general, **trace-l2** first tries to use the IP address of the virtual routing interface that is associated with a VLAN. If the virtual routing interface is not available, it then uses the loopback address. If both addresses are not available, it displays MAC address only.

The *input* and *output* ports show the path of the hops. Hop 3 has no output port because it is the destination.

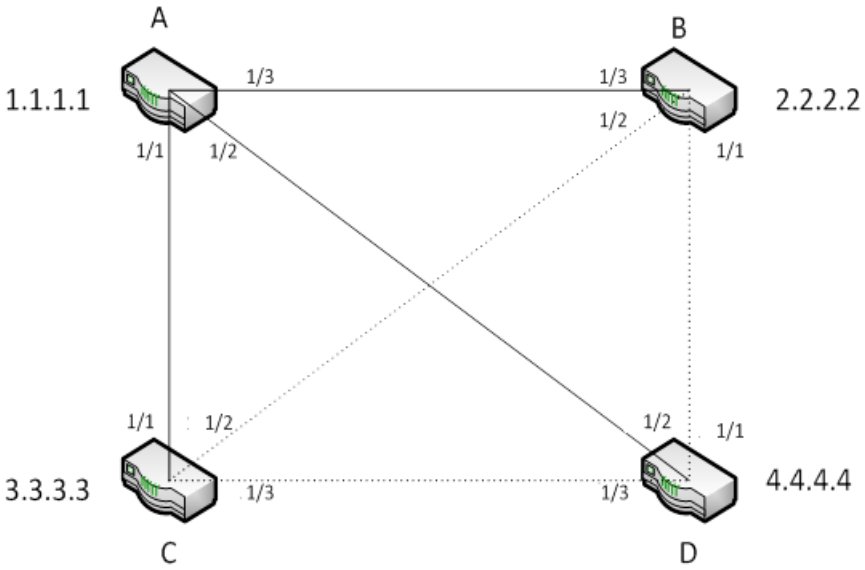
The *microsec* column is the round trip time (sum of the time) to and from the previous hop. For example, 316 microsec for hop 1 is the time from the source to hop 1 and from hop 1 to the source. One way time is not available because the tracel2 protocol does not synchronize the clocks between hops.

The **comment** column shows the Layer 2 protocol used on the input port. If a destination address is not specified or the destination does not exists, trace-l2 collects L2 topology information which can be displayed by issuing a **trace-l2 show** command.

Trace-L2 use case

Consider a mesh type topology with nodes A, B, C and D as shown in the figure below with all the shown ports on all the DUTs configured on vlan 10 and enabled with RSTP for loop resolution.

FIGURE 7 Sample Trace-L2 topology



With RSTP configured, device A is elected as the root bridge after convergence. The loop is resolved and resultant topology appears as shown in the figure above, with links between C and D, B and D and B and C blocked (shown with dotted lines). The trace-l2 protocol is enabled on a VLAN. You can trace the traffic path of a packet using following command on each device.

Displaying Layer 2 path information

Displaying Layer 2 path information on device A

Since device A is the RSTP root bridge, it is directly connected to the rest of the devices B, C, and D. So, enabling L2-trace to find the traffic path from A to B, C and D gives the following output.

```
device# trace-l2 vlan 10 2.2.2.2
trace-l2 reply vlan 10 from e1/3, 2.2.2.2, total round trip = 988 microsec
  hop input     output IP and/or MAC address       microsec comment
  1   e1/3         2.2.2.2 748e.f82b.a800           988     802-1w

device# trace-l2 vlan 10 3.3.3.3
trace-l2 reply vlan 10 from e1/1, 3.3.3.3, total round trip = 574 microsec
  hop input     output IP and/or MAC address       microsec comment
  1   e1/1         3.3.3.3 748e.f85a.0100           574     802-1w

device# trace-l2 vlan 10 4.4.4.4
trace-l2 reply vlan 10 from e1/1/2, 4.4.4.4, total round trip = 711 microsec
  hop input    output IP and/or MAC address       microsec  comment
  1   e1/2         4.4.4.4 748e.f85c.0800           711     802-1w
```

Displaying Layer 2 path information on device C

Since device C has link enabled only to device A (root bridge) and no links enabled to devices B and D, enabling L2-trace to find the traffic path from C to A, B and D generates the following output.

```
device# trace-l2 vlan 10 1.1.1.1
trace-l2 reply vlan 10 from e1/1, 1.1.1.1, total round trip = 546 microsec
  hop input    output IP and/or MAC address     microsec   comment
  1   e1/1         1.1.1.1 001b.edaf.7800          546    802-1w

device# trace-l2 vlan 10 2.2.2.2
trace-l2 reply vlan 10 from e1/1, 2.2.2.2, total round trip = 973 microsec
  hop input  output IP and/or MAC address       microsec   comment
  1   e1/1  e1/1  1.1.1.1 001b.edaf.7800          643     802-1w
  2   e1/2       2.2.2.2 748e.f82b.a800          330     802-1w

device# trace-l2 vlan 10 4.4.4.4
trace-l2 reply vlan 10 from e1/1, 4.4.4.4, total round trip = 811 microsec
  hop input  output IP and/or MAC address       microsec   comment
  1   e1/1   e1/1  1.1.1.1 001b.edaf.7800          516     802-1w
  2   e1/3        4.4.4.4 748e.f85c.0800          295     802-1w
```

Displaying Layer 2 topology information

To display information about the Layer 2 topology, first issue the **trace-l2 vlan** command. Then issue the **trace-l2 show** command as shown in the following example.

Displaying Layer 2 topology information on device B

Device B has link enabled only to device A (root bridge) and no direct links enabled to devices C and D. So, when the topology is probed from device B, the output shows two traffic paths for vlan 10 to reach C and D through A as shown below.

```
device# trace-l2 vlan 10
Vlan 10 L2 topology probed, use "trace-l2 show" to display

device# trace-l2 show
Vlan 10 L2 topology was probed 6 sec ago, # of paths: 2
path 1 from e1/3, 2 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/3      e1/3  001b.edaf.7846              999   802-1w
  2   e1/1        748e.f85c.080d                386   802-1w
path 2 from e1/3, 2 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/3     e1/3  001b.edaf.7846              1098  802-1w
  2   e1/2        748e.f85a.010b                500   802-1w
```

Displaying Layer 2 topology information on device D

Device D has link enabled only to device A (root bridge) and no links enabled to device B and C. So, when the topology is probed from device D, the output shows two traffic paths for vlan 10 to reach B and C through A as shown below.

```
device# trace-l2 vlan 10
Vlan 10 L2 topology probed, use "trace-l2 show" to display

device# trace-l2 show
Vlan 10 L2 topology was probed 5 sec ago, # of paths: 2
path 1 from e1/2, 2 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/2        e1/2  001b.edaf.783c           1088   802-1w
  2   e1/1           748e.f85a.010b              292    802-1w
path 2 from e1/2, 2 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/2        e1/1/2  001b.edaf.783c         1109   802-1w
  2   e1/3           748e.f82b.a8a6              326    802-1w
```

NOTE
The trace-l2 show command does not display a path if the path is a subset of another path. Therefore, the number of paths displayed could be fewer than the number of devices.

Displaying Layer 2 loop information

In this topology example, a loop is simulated by disabling spanning-tree on 1/1/2 in device C which puts the port from **Discarding** to **Forwarding** state. When the **trace-l2 vlan** command is issued, the following message is displayed.

```
device# trace-l2 vlan 10

*** Warning! The following 3 hops form a loop in vlan 10
  hop input  output IP and/or MAC address       microsec comment
  1                    001b.edaf.7800
  2   e1/3             748e.f82b.a8a6                 802-1w
  3   e1/2             748e.f85a.0113                 STP, *** e1/1/2 disabled

Vlan 10 L2 topology probed, use "trace-l2 show" to display
```

The **trace-l2 show** command returns the following output.

```
device# trace-l2 show

*** Warning! The following 3 hops form a loop in vlan 10
  hop input  output IP and/or MAC address       microsec comment
  1               001b.edaf.7800
  2   e1/3        748e.f82b.a8a6                  802-1w
  3   e1/2        748e.f85a.0113                  STP, *** e1/1/2 disabled

Vlan 10 L2 topology was probed 144 sec ago, # of paths: 3
path 1 from e1/2, 1 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/2              748e.f85c.080d          946    802-1w
path 2 from e1/1, 2 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/1   e1/2  748e.f85a.010b                1528   802-1w
  2   e1/2               748e.f82b.a8a2                413 802-1w
path 3 from e1/3, 2 hops:
  hop input  output IP and/or MAC address       microsec comment
  1   e1/3   e1/2  748e.f82b.a8a6                1480    802-1w
  2   e1/2         748e.f85a.0113                396     STP, *** e1/1/2 disabled
```

Port Mirroring

Port mirroring is used to send packets entering or exiting in one port to another port or LAG. Mirroring can be done in ingress, egress, or in both directions.

Port mirroring is enabled using the **monitor session** command. This command enables the session for monitoring. You can further set the source, destination and direction. Destination can be either ethernet interface or port-channel. Destination port can be on same chip, different chip, or on a different line card. For more information on the **monitor session** command, refer the *Brocade SLX OS Command Reference* for the SLX 9850 Router.

NOTE
To add destination interface for monitor, all the protocols such as "LLDP" must be disabled on the destination interface.

The maximum number of session IDs configurable per chassis using Brocade SLX-OS is 512. A maximum of 15 different destination ports can be configured per Jericho chip.

RASLOG error message will be displayed on console if mirror Id is not available. If you try to mirror to a destination for which mirror id is already allocated on the chip, the configuration will be allowed. There is no difference in mirroring based on speeds of the interface such as 10G or 40G interface. So, the mirroring feature works same on interfaces with different speeds.

NOTE
When mirroring is done across Line cards with different speeds, the regular limitations of forwarding is applied. For example, when the traffic is mirrored from a 40G port to a 10G port, the traffic exceeding 10G rate is dropped by the10G interface.

Configuring port mirroring

Execute the following steps to configure port mirroring.

1. Enter the ethernet interface configuration mode.

```
device(config)# interface ethernet 8/2
device(conf-if-eth-8/2)
```

2. Issue the **lldp disable** command to disable lldp.

```
device(conf-if-eth-8/2)# lldp disable
2016/08/22-06:47:13, [ONMD-1004], 959, M1 | Active | DCE, INFO, SLX, LLDP is disabled on interface
Eth 8/2.
```

3. Exit the ethernet interface configuration mode.

```
device(conf-if-eth-8/2)# exit
device(config)#
```

4. Issue the **monitor session** command.

```
device(config)# monitor session 1
2016/08/22-06:47:17, [NSM-1031], 960, M1 | Active | DCE, INFO, SLX, Session 1 is created.
```

5. Add the source and destination interface using the **source ethernet** command to monitor session.

```
device(config-session-1)# source ethernet 8/1 destination ethernet 8/2 direction rx
2016/08/22-06:47:29, [NSM-1034], 961, M1 | Active | DCE, INFO, SLX, Session 1 configuration is added.
device(config-session-1)# end
```

NOTE

Destination can either be ethernet interface or port-channel.

Following is a sample **show monitor** command output.

```
device# show monitor session 1

Session                : 1
Description            : [None]
State                  : Enabled
Source Interface       : Eth 8/1 (Up)
Destination Interface  : Eth 8/2 (Down)
Direction              : Rx
device#
```

Network Elements Telemetry

Network elements telemetry overview

Network Elements Telemetry is a mechanism by which important data and other measurements are collected at regular intervals and transmitted to external equipment for monitoring and analysis purposes.

In the case of network elements, telemetry data includes interface statistic counters and metrics, such as memory utilization and processor utilization. The device that receives this telemetry data is called a telemetry collector. The SLX-OS device that gathers the data required is called a telemetry server. The collector devices run analytics applications that process the data and provide visibility into the performance of the network.

Streaming of telemetry data

The telemetry data that is collected on the network elements must be sent to the collectors using an efficient mechanism called streaming telemetry.

Streaming telemetry is supported using the following two approaches:

- SLX-OS acting as a gRPC server
- SLX-OS acting as a TCP client

Encoding formats

The only supported encoding format is Google Protocol Buffers (GPB).

Telemetry profiles

A telemetry profile contains one or more telemetry objects along with the streaming interval. There are two basic types of telemetry profiles: system profile and interface profile.

System profile

The system telemetry profile contains the system-related telemetry data along with the streaming interval. The default system profile contains all available counters and a sampling interval of 60 seconds. The default system profile can be customized to contain a subset of the counters and a streaming interval of your choice.

Interface profile

The interface telemetry profile contains the telemetry data related to the physical interface and the corresponding streaming interval. The provided default interface profile contains all available interface counters and a streaming interval of 30 seconds. Users can customize this profile to contain any subset of the interface-level counters along with a streaming interval. Additionally, you must configure a list of designated interfaces before using this profile.

Supported telemetry data

The following system-related telemetry data classifications are supported.

System data

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

Interface counters

Interface counters are supported on physical interfaces only.

- 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

Streaming telemetry data using a gRPC server

In the gRPC approach, the device acts as a server listening on port 50051. The Google gRPC server is integrated with SLX-OS to handle the RPC requests from the client device on this port.

The gRPC server always listens on mgmt.-vrf. The gRPC server can stream over an unsecured TCP connection or over a secure SSL connection.

Streaming telemetry data to a collector profile

In the collector profile, the device acts as a client. A collector becomes the destination for the telemetry data streamed from the device.

Once the collector is activated, the device streams data in the configured encoding format at the specified interval.

In addition to the collector configuration on the device, the server profile must be configured on the remote host server (the collector) using the IP address, port, and transport method (TCP or SSL) of the profile to process telemetry records.

When configuring the collector using a collector profile, the telemetry profile must be specified along with the encoding format.

The collector profile defines collector-related information as:

- Destination IP address and port number
- Encoding format in which data must be sent (currently supported in GPB format only)
- Telemetry profiles

Telemetry Secure Certificate Management

Telemetry supports secure monitoring through SSL transport security.

1. In privileged EXEC mode, enter **configure terminal** to enter global configuration mode.

   ```
   device# configure terminal
   Entering configuration mode terminal
   ```

2. Enter the **telemetry server** command to enter telemetry server configuration mode.

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

3. Enter the **activate** command to activate the telemetry server, which initiates all gathering and streaming of telemetry information.

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

4. To manage secured connections, enter the **do telemetry client-cert generate** command to generate the telemetry SSL certificates used by the server and client.

   Note: Use the **do telemetry client-cert delete** command to remove a certificate.

   ```
   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 collectors.

```
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. For secure data transfer on the transport layer, the **transport** command provides an option of TLS using SSL as the encryption mechanism.

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

The following is a complete telemetry server configuration example with secure connection.

```
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
```

Configuring telemetry profiles

Configuring telemetry profiles requires the **telemetry profile** command, which allows for editing and enabling the telemetry configuration.

Two preconfigured default profiles support monitoring and collecting telemetry data. These profiles contain all the supported streaming attributes. You can customize the profiles by removing unrequired attributes, or modifying the interval delay. This procedure applies to either profile equally. The profiles are:

- ***system-utilization: default_system_utilization_statistics*** This profile can be used as is, since there are no additional required parameters. If required, the interval or other attributes can be removed.
- ***interface: default_interface_statistics*** This profile can be used for streaming after specifying the required interfaces.

The profile can be modified using **add** and **interval** commands. The **add** command allows to add or remove attributes to profile. The **interval** command sets the monitoring interval for the profile in seconds. In case any filters are applicable to the profile, those are available as additional commands. For example, the **interface** command specifies the range of physical interfaces to monitor for default_interface_statistics profile.

The profiles cannot be deleted, but each attribute can be removed using the **no add** command.

1. In privileged EXEC mode, enter **configure terminal** to enter global configuration mode.

```
device# configure terminal
Entering configuration mode terminal
```

2. Enter the **telemetry profile** to enter telemetry profile configuration mode.

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

3. Enter the **interface** command to designated interface range to monitor.

   For information on all the attributes of the **interface** refer to the *Brocade SLX-OS Command Reference* for the SLX 9850 and SLX 9540 Switches.

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

4. Enter the **interval 30** command to set the monitoring interval to 30 seconds. Repeat this step for additional attributes.

   For information on all the attributes of the **interval** refer to the *Brocade SLX-OS Command Reference*

   for the SLX 9850 and SLX 9540 Switches.

```
device(config-telemetry-profile)# interval 30
```

5. Enter the **exit** command to exit the configuration mode and save the configuration.

```
device(config-telemetry-profile)# exit
device(config)#
```

The following is a complete telemetry profile configuration example.

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

Configuring the telemetry collectors

Telemetry collectors are configured from the telemetry collector configuration mode using the **telemetry collector** command.

Configure the telemetry profiles before configuring the telemetry collector.

1. In privileged EXEC mode, enter **configure terminal** to enter global configuration mode.

```
device# configure terminal
Entering configuration mode terminal
```

2. Enter the **telemetry collector** command to enter telemetry collector configuration mode. A telemetry collector name can be a string of up to 32 characters (alphanumeric characters and underscores).

   The create function occurs when the specified telemetry collector name does not exist; otherwise, the update function occurs. Update operations are not allowed while the collector is activated. The collector must be deactivated (no activate mode) before modifications can be made to an existing configuration.

```
device(config)# telemetry collector collector_1
device(config-telemetry-collector_collector_1)#
```

3. Enter the **ip port** command to configure the IP address and port.

```
device(config-telemetry-collector_collector_1)# ip 10.168.112.10 port 1
```

4. Enter the **profile** command to add the telemetry profiles.

```
device(config-telemetry-collector_collector_1)# profile system-utilization
default_system_utilization_statistics
device(config-telemetry-collector_collector_1)# profile interface default_interface_statistics
```

5. Enter the **activate** command to activate the telemetry collector. The telemetry server must be active at the specified IP address and port in order for the data to be collected.

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

6. Enter the **show telemetry collector** command to display the status of a specified telemetry collector.

```
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
!
```

7. Enter the **show telemetry collector status** command to display the status of currently active telemetry collector sessions..

```
device(config-collector-collector_1)# do show telemetry collector status

Activated Collectors:
---------------------
Name                      IP Address:Port            Streaming/Connection Status
--------------------      ------------------       ---------------------------
Collector_3333            10.70.12.112:33333          starting_profiles
Collector_4444            10.70.12.112:44444          streaming
Collector_2345            10.70.12.112:33333          streaming_errored
```

The following is a complete telemetry collection configuration example.

```
device# configure terminal
Entering configuration mode terminal
device(config)# telemetry collector collector_1
device(config-telemetry-collector_collector_1)# ip 10.168.112.10 port 1
device(config-telemetry-collector_collector_1)# profile system-utilization
default_system_utilization_statistics
device(config-telemetry-collector_collector_1)# profile interface default_interface_statistics
device(config-collector-collector_1)# activate
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
```

Configuring telemetry servers

A telemetry server is configured from telemetry server configuration mode using the **telemetry server** command.

1. In privileged EXEC mode, enter **configure terminal** to enter global configuration mode.

   ```
   device# configure terminal
   Entering configuration mode terminal
   ```

2. Enter the **telemetry server** command to enter telemetry server configuration mode.

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

3. Enter the **activate** command to activate the telemetry server, which initiates all gathering and streaming of telemetry information.

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

4. 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 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
   ```

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 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
```

Hardware Monitoring

Hardware monitoring overview

Hardware monitoring allows you to monitor CPU and memory usage of the system, interface and optic environmental status, and security status and be alerted when configured thresholds are exceeded.

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)

The System Resource Monitoring (SRM) provides periodic, continuous check on system-wide memory and per-process memory usages in an active running switch and provide warnings to users regarding abnormally high memory usage.

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

Execute the following steps to configure 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 4 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

Alerts can be set 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

The Line card software polls each port periodically to detect the presence of optic. Once an optic is detected, it reads the erasable programmable read only memory (EPROM) to determine if it is Brocade certified. The data is read periodically to monitor the health. If the line card 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 Brocade are not monitored. However these port links are not prevented form coming up.

NOTE
Optical monitoring is supported on the 72X10G and the 60X40G line card.

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

TABLE 5 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 Brocade certified optics, optical monitoring is performed using Fabric Watch (FW).

Optical monitoring in Fabric Watch

For optical monitoring, Fabric Watch (FW) is enabled by default. You can view the default optical monitoring thresholds using the **show defaults threshold sfp type** command where the SFP types are as follows.

TABLE 6 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

TABLE 6 Optical monitoring thresholds (continued)

SFP type	Default threshold
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
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

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

You can view the optical monitoring default values by entering **show defaults threshold** followed by the SFP type.

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

To view the area wise optical monitoring current status and value, run the **show threshold monitor sfp all area** command.

```
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

Support for T-SFP+ optical transceiver module is provided through port configuration.

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

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

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-monitorsfp pause** command.

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

Optic thresholds

You can customize Opticthresholds 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.

TABLE 7 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
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

TABLE 7 Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
	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
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
100GLR	Temperature	C	-5	75

TABLE 7 Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
	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
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

TABLE 7 Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
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
100GESR	40GLM	Temperature	-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
100GAOC	40GLM	Temperature	-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

Threshold values

High and low threshold values are the values at which potential problems might occur. For example, in configuring a temperature threshold for SFPs, you can select the temperatures at which a potential problem can occur because of overheating or overcooling.

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.

Cyclic redundancy check (CRC)

Cyclic redundancy check (CRC) polls CRC errors for each port in the configured polling interval.

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
```

For more information on commands, refer the *SLX-OS Command Reference* .

High and Low watermarks for port utilization

This feature maintains a database of high and low watermarks of port bandwidth utilization in terms of Mega Bits Per Second (MBPS) and Packets Per Second (PPS).

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 by the line card (LC). 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 line 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.

Beacon LED support

Beacon LEDs are supported on SLX 9850 and SLX 9540 platforms.

Beacon LED can be configured in following two ways:

- **Chassis based beacon configuration**: If configured, all interfaces on all the line cards of the chassis will blink at a rate of 1 blink per second. This is configured using the **beacon enable chassis** command. RASLOG messages will be displayed for both chassis beacon enable and disable.
- **Interface/port-channel based beacon configuration**: If configured, only the specific ethernet interface or port-channel will blink at a rate of 1 blink per second. This is configured using the **beacon enable interface** command.

For more information on the configuration commands, please refer the Brocade SLX-OS Command Reference supporting the SLX 9850 and 9540 Devices.

Remote Monitoring

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 RMON Ethernet group statistics collection

You can collect RMON Ethernet group statistics on an interface. RMON alarms and events must be configured for you to display collection statistics. By default, RMON Ethernet group statistics are not enabled.

Ethernet group statistics collection is not supported on ISL links.

To collect RMON Ethernet group statistics on an interface, perform the following steps from privileged EXEC mode.

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

```
device# configure terminal
```

2. Enter the **interface** command to specify the interface type and slot/port number.

```
device(config)# interface ethernet 1/1
```

3. Configure RMON Ethernet group statistics on the interface.

```
device(conf-if-eth-1/1)# rmon collection stats 200 owner john_smith
```

4. Return to privileged EXEC mode.

```
device(conf-if-eth-1/1)# end
```

5. Enter the **copy** command to save the running-config file to the startup-config file.

```
device# copy running-config startup-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

Certain interface counters, such as those for CRC errors, may not be available by means of SNMP OIDs. In this case it is recommended that either RMON or CLI be used to monitor those statistics.

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 1/1
device(conf-if-eth-1/1)# rmon collection stats 2 owner admin
```

4. Use an appropriate RMON MIB for additional monitoring.
   For example, to obtain CRC statistics on a Brocade 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

System Monitor provides customizable monitoring thresholds, which allow you to monitor the health of each component of a device. Whenever a device component exceeds a configured threshold, System Monitor automatically provides notification by means of e-mail or RASLog messages, depending on the configuration.

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:

- **LineCard**—Displays the threshold for the line card.
- **MM**—Displays the threshold for the management module.
- **SFM**—Displays the threshold for the switch fabric module device.
- **cid-card**—Displays the threshold for the chassis ID card component.
- **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.

NOTE
CID cards can be faulted and removed. The system continues to operate normally as long as one CID card is installed. If both CID cards are missing or faulted, the device will not operate.

Monitored FRUs

System Monitor monitors the absolute state of the following FRUs:

- Fan
- Power supply
- CID card
- Line 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

Switch Fabric Module (SFM), and Traffic Manager (TM) error interrupts are logged in RASLOG.

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.

NOTE
For command details, refer to the *Brocade SLX-OS Command Reference*.

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 82.)

1. Issue the **configure terminal** command to enter global configuration mode.
2. Change **down-threshold** and **marginal-threshold** values for the SFM.

```
device(config)# system-monitor sfm threshold down-threshold 3 marginal-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 *Brocade SLX-OS Command Reference* Brocade SLX-OS Command Reference supporting the SLX 9850 and 9540 Devices.

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.brocade.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

You can view the optical monitoring default values by entering **show defaults threshold** followed by the SFP type.

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

To view the area wise optical monitoring current status and value, run the **show threshold monitor sfp all area** command.

```
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**.

```
device# show system monitor
** ** System Monitor Switch Health Report **
               Switch status            : MARGINAL
               Time of Report           : 2016-08-18 18:10:09
               Power supplies monitor   : HEALTHY
               Temperatures monitor     : HEALTHY
               Fans monitor             : HEALTHY
               CID-Card monitor         : HEALTHY
               MM monitor               : HEALTHY
               LC monitor               : HEALTHY
               SFM monitor              : MARGINAL
               Flash monitor            : HEALTHY
```

Logging and tracing

Overview

Logging and tracing involves, RASTrace, RASLog, AuditLog and Syslog.

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 MMVM/linux shell for usage information.

RASTrace, RASLog, AuditLog and Syslog are detailed in the following section of the docuemnt.

RASLog

RASLog subsystem provides centralized logging mechanism. RASLog messages log system events related to configuration changes or system error conditions.

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 8 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 *Brocade SLX-OS Message Reference*.

Trace Rotation

The trace rotation feature overcomes the challenges of trace wraparound by automatically dumping the trace content into a file when the number of entries reaches the watermark. This saves the trace entries from getting lost because of the wraparound.

Trace rotation is configured per module basis. The trace rotation utility allows you to enable or disable at run time. If a module wants to enable trace rotation, the rotation flag field at the trace configuration file is set to 1. To disable trace rotation, the flag field is set to 0.

NOTE

For key trace modules, trace rotation is enabled by default at the configuration file. The key trace modules are available at

```
/vobs/projects/springboard/fabos/bccb/utils/trace/rf_keymodules.conf
```

The following trace categories do not have trace rotation enabled:

- Snapshot module trace: These modules have very high logging traffic and trace wraparounds happen every couple seconds.
- Modules with trace entry size configuration greater than 64.
- Non key module trace.

AuditLog

AuditLog messages are classified into three types: DCM Configuration (DCMCFG), Firmware (FIRMWARE), and Security (SECURITY).

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 *Brocade SLX-OS Message Reference* .

Syslog

The syslog protocol allow devices to send event notification messages across IP networks to event message collectors, also known as syslog servers.

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, VRF-name and port are the parameters used.

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="SLX9850-4"][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 *Brocade SLX-OS Message Reference* for the SLX 9850 and SLX 9540 Devices.

.

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 **certutil 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.

```
device# certutil import syslogca directory /usr/ldapcacert/ file cacert.pem protocol SCP host 10.23.24.56
user jane password
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 cert-util syslogcacert** command.

This example displays the syslog CA certificates.

```
device# show cert-util syslogcacert
```

Verifying syslog CA certificates

To test whether a syslog CA certificate has been imported on the device, in privileged EXEC mode, enter the **no certutil 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

```
device# no certutil syslogcacert
% Error: syslog CA certificate does not exist.
```

Example for when a syslog CA certificate exists on the device

```
device# no certutil syslogcacert
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 certutil syslogca** command. You will be prompted to confirm that you want to delete the syslog CA certificates.

This example deletes the syslog CA certificates.

```
device# no certutil syslogca
Do you want to delete syslogca certificate? [y/n]:y
Warning: All the syslog CA certificates are deleted.
```

sFlow

Overview

The sFlow protocol is an industry-standard technology for monitoring high-speed switched networks.

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

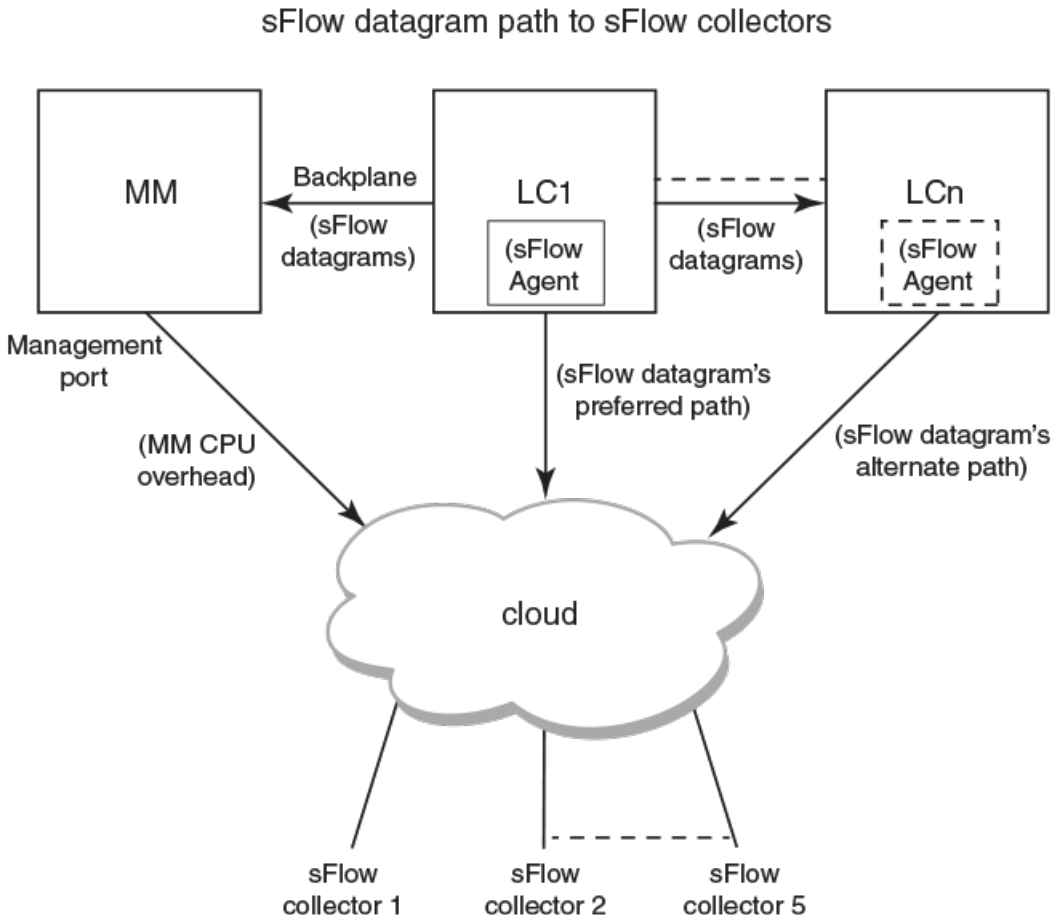
NOTE

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.

sFlow Datagram Flow

The following diagram depicts the three possible paths that a given sFlow datagram can take to the sFlow collectors, based on the route to the destination (sFlow collector).



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 sFlow feature support matrix for this release.

TABLE 9 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
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	Cannot be configured through CLI. Management CP IP is always 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.

Configuring sFlow

sFlow configuration involves global configuration and configuration on interfaces. Following are the steps involved at a high level.

- 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.

Configuring sFlow globally

Execute the following steps to configure 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
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.

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.

Configuration example

Global configuration

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
```

Offline diagnostics

Offline diagnostics

Offline diagnostics is supported on Line Card (LC) and Switch Fabric Element.

To run the offline tests on LC or MM, system must be partitioned with the new model as described in the SLX OS installation page. This requires images to be present on the target, to get access to the partition containing the offline-diag binary and the components of offline-diag that are required for executing the offline-diag.

On MM (Switch Fabric Element), following are the tests supported:

- TR 5 – MBIST Test (HW Test of memories)
- TR 131 – DFE Snake Test (with looped back configuration)

On LC and MM (Integrated TM & PP), following are the tests supported:

- TR 8 – Memory Flip/Flop Test
- TR 140 – DDR BIST (Two data set patterns)

Executing offline diagnostics test on 9845 LC

Perform the following steps to run the offline diagnostics tests on 9845 LC.

> **NOTE**
> In this example, the offline diagnostics test is run on line card lc3 of 9845.

1. Issue the **offlinediagon** command on the MM to transition the specific line card to run offline diagnostics tests.

```
device# offlinediagon lc3
```

2. On 9850 MM, issue the **slotshow** command to view the slot status.

```
device# slotshow
```

3. Issue the **rconsole** command to connect to the line card for which you require to perform offline diagnostics tests from MM.

```
device# rconsole.sh 3
```

> **NOTE**
> This command connects to the line card L3.

4. Login to the session using the standard root credentials.

5. Issue the **offlinediag** command to execute the test on the line card.

```
device# offlinediag
```

6. Press **Ctrl-\ q** sequence to disconnect from the line card for returning to main mm console.
7. Issue the **slotshow** command to view the slots available.

```
device# slotshow
```

8. Issue the **offlinediagoff** command to restart the line card to normal application state.

```
device# offlinediagoff lc3
```

9. Issue the **offlinediagget lc3** to get the offline diagnostics results from the linecard to the mm folder.

```
device# offlinediagget lc3
```

10. Issue the **offlinediagstatus** to check the status of the offline diagnostics for the line card.

```
device# offlinediagstatus lc3
```

11. Issue the **offlinediagshowlog** command to view the logs of the test results for the linecard.

```
device# offlinediagshowlog lc3
```

Executing offline diagnostics test on 9850 MM

Perform the following steps to run the offline diagnostics tests on 9850 MM.

NOTE
In this example, the offline diagnostics test is run on
mm1.

1. Issue the **mmdiagon** command on the MM to transition the specific MM card to run the offline diagnostic tests. This would reset the mm and provide console to offline diagnostics test.

```
device# mmdiagon mm1
```

2. Login using standard root credentials
3. Issue the **offlinediag** command to execute the offline diagnostics test.

```
device# offlinediag
```

4. Issue the **reboot** command to restart the MM card to bring it back to the normal application mode.

```
device# reboot
```

5. Issue the **offlinediagget** command to get the logs of the offline diagnostics tests of MM performed.

```
device# offlinediagget mm1
```

6. Issue the **offlinediagstatus** command to display the summary of the test results.

```
device# offlinediagstatus mm1
```

7. Issue the **offlinediagshowlog** command to view the logs of the rest result.

```
device# offlinediagshowlog mm1
```

Executing offline diagnostics test on 9540 MM

Perform the following steps to run the offline diagnostics tests on 9540 MM.

1. Issue the **offlinediagon** command on the MM to transition the MM card to run the offline diagnostic tests. This would reset the mm and provide console to offline diagnostics test.

```
device# offlinediagon
```

2. Login using standard root credentials
3. Issue the **offlinediag** command to execute the offline diagnostics test.

```
device# offlinediag
```

4. Issue the **reboot** command to restart the MM card to bring it back to the normal application mode.

```
device# reboot
```

5. Issue the **offlinediagget** command to get the logs of the offline diagnostics tests of MM performed.

```
device# offlinediagget
```

6. Issue the **offlinediagstatus** command to display the summary of the test results.

```
device# offlinediagstatus
```

7. Issue the **offlinediagshowlog** command to view the logs of the rest result.

```
device# offlinediagshowlog
```