CONFIGURATION GUIDE

Brocade SLX-OS Monitoring Configuration Guide, 16r.1.00

Supporting the Brocade SLX 9850 Router

53-1004416-01
31 August 2016

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 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, by telephone, or by e-mail. 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	E-mail
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	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

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 16r.1.00, 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

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

What's new in this document

This document supports the following features introduced in Brocade SLX-OS 16r.1.00:

- enter feature name here
- enter feature name here

For complete information, refer to the *SLX-OS Release Notes*.

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.

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

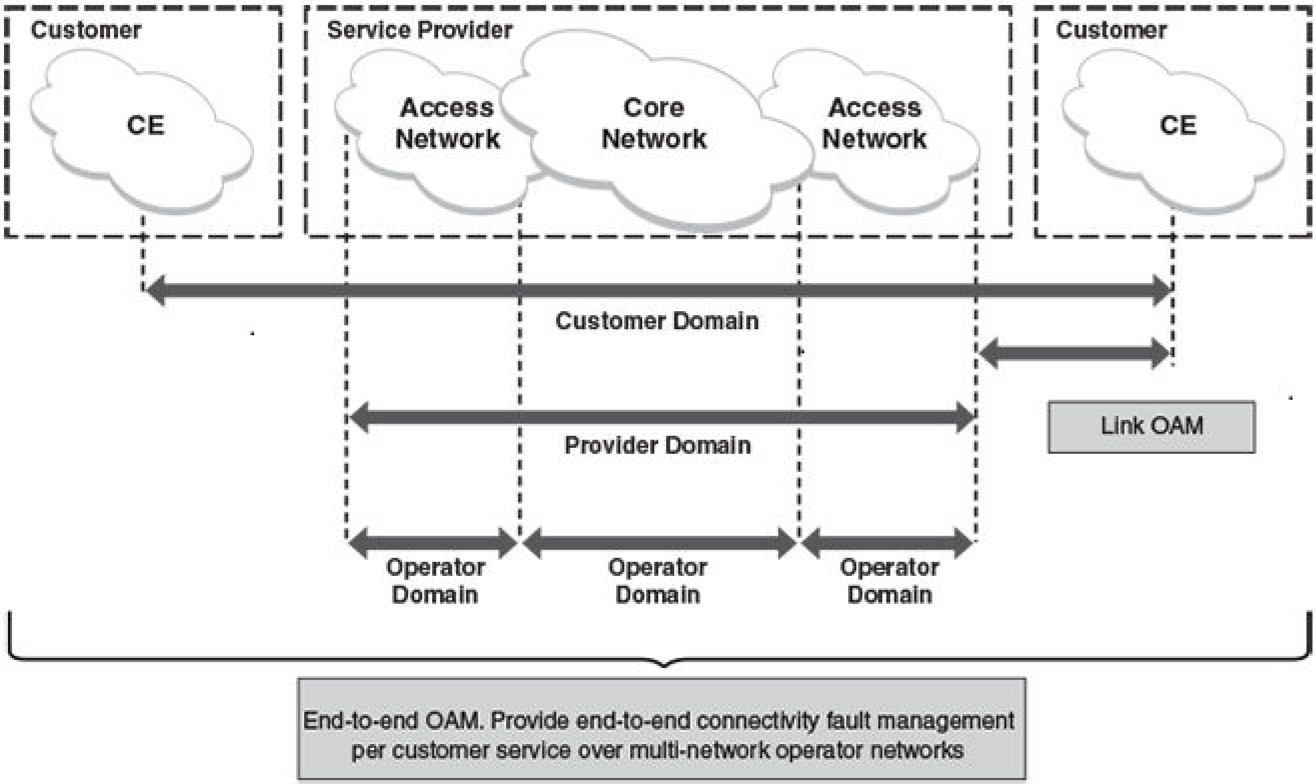
Bridges are increasingly used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM provides capabilities for detecting, verifying and isolating connectivity failures in such networks.

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 (MD)

A Maintenance domain is part of a network controlled by a single operator. In Figure 1 on page 12, we have customer domain, provider domain and operator domain.

Maintenance Domain level (MD level)

The MD levels are carried on all CFM frames to identify different domains. For example, in Figure 1 on page 12, 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 (MA)

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

Maintenance End Point (MEP)

MEP is located on the edge of an 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 (MIP)

MIP is located within a 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.

Configuring IEEE 802.1ag CFM

Enabling or disabling CFM

To enable or disable the CFM protocol globally on the devices and enter into the CFM Protocol Configuration mode, enter the following command.

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

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

Creating a Maintenance Domain

A Maintenance Domain 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.

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

Each Maintenance Domain can be separately administered.

The **domain-name** command in CFM protocol configuration mode creates a maintenance domain with a specified level and name and enters the Specific Maintenance Domain mode specified in the command argument.

```
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.

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

   ```
   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 mode to the specific maintenance association mode.

2. Set the time interval between two successive Continuity Check Messages (CCMs) that are sent by MEPs in the specified Maintenance Association, use the **ccm-interval** 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)#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 Maintenance Association mode.

   ```
   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 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(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(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.

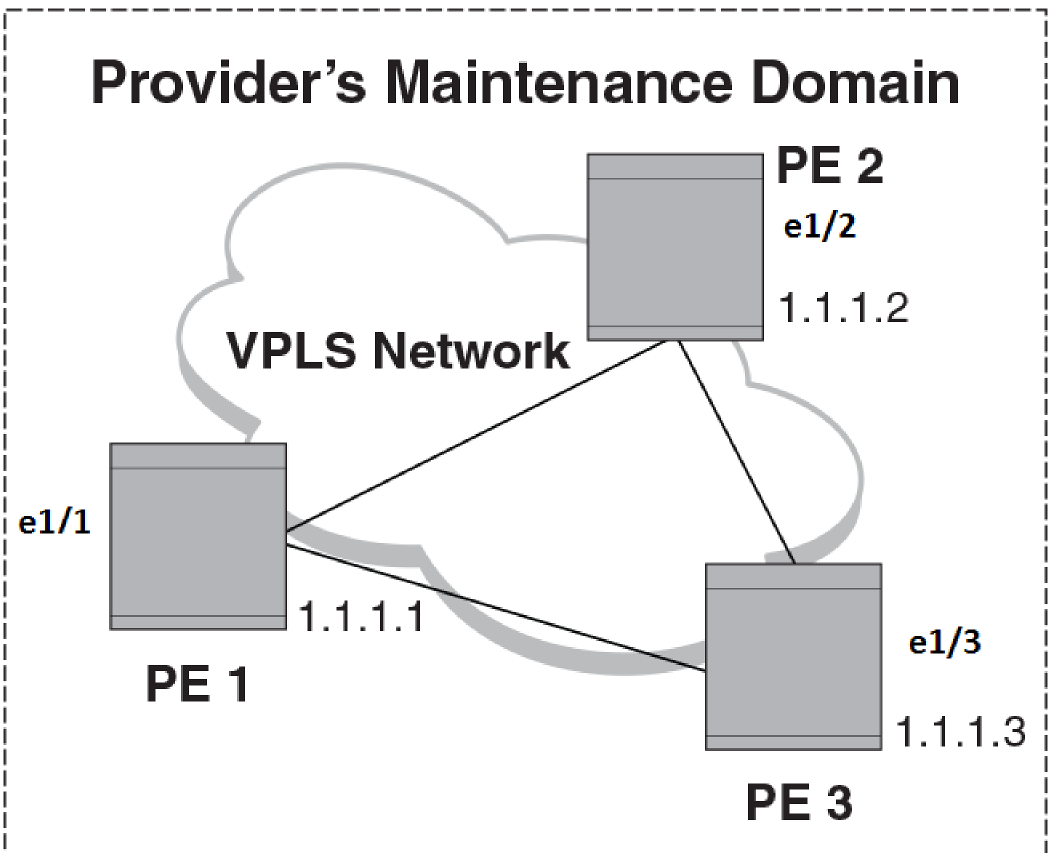
Monitoring the status of devices in a VPLS network in a Provider's Maintenance Domain

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 2 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.

Show commands

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

Show cfm

Use the **show cfm** command to display the cfm configuration.

Syntax: show cfm

```
Domain: md1
Level: 7
  Maintenance association: ma1
  MA Index: 100
  CCM interval: 10000 ms
  VLAN ID: 100
  Priority: 7
  MEP   Direction  MAC               PORT        PORT-STATUS-TLV
  ====  =========  =========         ====        ===============
  1     DOWN       609c.9f02.d548    Eth 1/2     N
  MIP   VLAN/Peer         Port       Level   MAC
```

```
===    =========          ====      =====    ===
       100                Eth 1/72  7        609c.9f02.d542
```

NOTE
For the **show cfm** command to generate output, CFM should first be enabled in Protocol Configuration mode.

Show cfm connectivity

Use the **show cfm connectivity** command to display the cfm connectivity configuration.

show cfm connectivity

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

```
Domain: md2
Domain: md1
Level: 7
  Maintenance association: ma1
  MA Index: 100
  CCM interval: 10000
  VLAN ID: 100
  Priority: 7
    MEP Id: 1
    MEP Port: Eth 1/2
      RMEP  MAC             VLAN/PEER         PORT      STATE
      ====  ===             =========         ====      =====
      19    0000.0102.0304  100               Eth 1/2   OK
```

NOTE
For the **show cfm connectivity** command to generate result, CFM should first be enabled in the Protocol Configuration mode.

Show cfm brief

Use the **show cfm brief** command to display the CFM brief output.

```
device# show cfm brief
Domain: md1
Level: 7  Num of MA: 1
  Maintenance association: ma1
  MA Index: 100
  CCM interval: 10000 ms
  VLAN ID: 100
  Priority: 7
  Num of MEP: 1  Num of RMEP: 1
  rmepfail: 1 rmepok: 0
```

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.

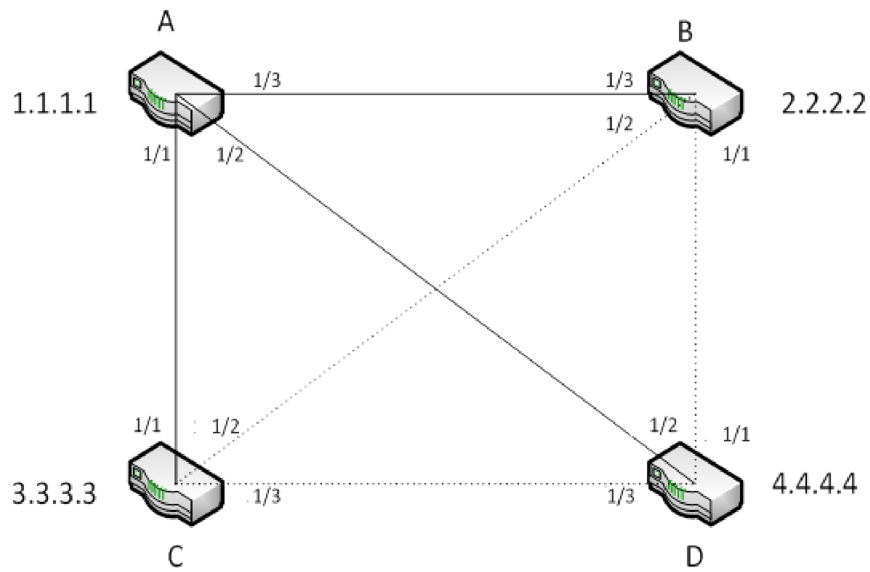
The *microsec* column is the round trip time (sum of the time) to and from the previous hop. For example, 316 microsec for hop 1 is the time from the source to hop 1 and from hop 1 to the source. One way time is not available because the tracel2 protocol does not synchronize the clocks between hops.

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 3 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                792e.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.

If you try to configure more than 4 different destination ports on a particular Jericho chip, the configuration will fail. 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#
```

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.

Following are some of the specific functions which SRM offers:

- **Configuration**: SRM allows you to enable or disable the services, set threshold for high usage, and configure the how you must be notified when the threshold limit hit.
- **Light-weighted sampling**: SRM triggers a lighted-weighted sampling on system-wide and per-process memory usages at real-time, every 10 second. This allows the quick detection of high memory usage condition without imposing additional burden to the system or interfering with the switch's normal functionality.
- **Data logging**: SRM periodically logs detailed memory usage data at low frequency and archive them for a long period of time. By default, data is archived for a month. By default, the periodical logging rate for memory usage data is once in every hour. This is lower than the sampling rate, in order to minimize the impact to the overall system resource.

With the per-process memory monitoring service enabled, if the high memory usage threshold is crossed for any of the processes, a **warning** 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. This functionality is provided by the **resource-monitor** command. For more information on the command, please refer the Network OS Command Reference.

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. Reporting is also done in MAPS.

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 1 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.

To display the default values of thresholds and alert options, enter the **show defaults threshold** command, as in the following example for interfaces.

```
device# show defaults threshold interface type Ethernet

Type: GigE-Port
+--------+----------------------+----------------------+------+-------+
|        |    High Threshold    |    Low Threshold     |Buffer|Time   |
|Area    |Value | Above  | Below |Value | Above | Below |Value |Base   |
|        |      | Action | Action|      | Action| Action|      |       |
+--------+------+--------+-------+------+-------+-------+------+-------+
|MTC     |  300 | none   | none  |    12| none  | none  |     0|minute |
+--------+------+--------+-------+------+-------+-------+------+-------+
|CRCAlign|  300 | none   | none  |    12| none  | none  |     0|minute |
+--------+------+--------+-------+------+-------+-------+------+-------+
|Symbol  |    5 | none   | none  |     0| none  | none  |     0|minute |
+--------+------+--------+-------+------+-------+-------+------+-------+
|IFG     |  100 | none   | none  |     5| none  | none  |     0|minute |
+--------+------+--------+-------+------+-------+-------+------+-------+
MTC - Missing Termination Character
```

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 2 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 3 optical monitoring thresholds

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

TABLE 3 optical monitoring thresholds (continued)

SFP type	Default threshold
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

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
```

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 mypolicy
   ```

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 4 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
	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

TABLE 4 Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
	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	3700
	Power on hours	Hrs	0	0
40GSRINT	Temperature	C	-5	75
	RX power	uW	45	2188
	TX power	uW	0	0
	Current	mA	1	10
	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	25	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
	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	17

TABLE 4 Factory thresholds for optic types and monitoring areas (continued)

Optic type	Area	Unit	Low	High
	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

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.

Pausing and continuing threshold monitoring

By default, threshold monitoring is enabled.

To disable monitoring of a particular type, enter the **threshold-monitor [cpu |interface | memory | security | sfp] pause** command.

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

> NOTE
> Not all functions of the **threshold-monitor** command can be disabled. Continue to enter **?** at each level of the command synopsis to confirm which functions can be disabled.

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.

```
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. Enable the DCB interface.

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

4. Configure RMON Ethernet group statistics on the interface.

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

5. Return to privileged EXEC mode.

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

6. 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. First use the **clear counters all** command in global configuration mode.

   ```
   device# clear counters all
   ```

2. Then use **the clear counters rmon** command.

   ```
   device# clear counters rmon
   ```

3. Finally, 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.
- **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

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.

Based on the configured threshold, each component can be in a marginal state or a down state. If a component is in a marginal state or a down state, System Monitor generates a RASLog message to alert the user. It also generates a separate RASLog message for the overall health of the device.

SFM monitoring

Switch Fabric Module (SFM), Fabric Element (FE), 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 44.)

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. A single email configuration is applicable for all devices in a logical chassis cluster. For complete information on the **system-monitor-mail relay host** command, refer to the *Brocade SLX-OS Command Reference* .

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 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:

```
device(config)# system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name1.brocade.com
```

- To delete the mapping:

```
device(config)# no system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name1.brocade.com
```

- To change the domain name:

```
device(config)# system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name2.brocade.com
```

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:

```
device(config)# no system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name2.brocade.com
```

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
```

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 5 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*.

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 *Brocade SLX-OS Message Reference* for the SLX 9850 Router.

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 *Brocade SLX-OS Message Reference* for the SLX 9850 Router.

.

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** and **ACL based** (flow 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.

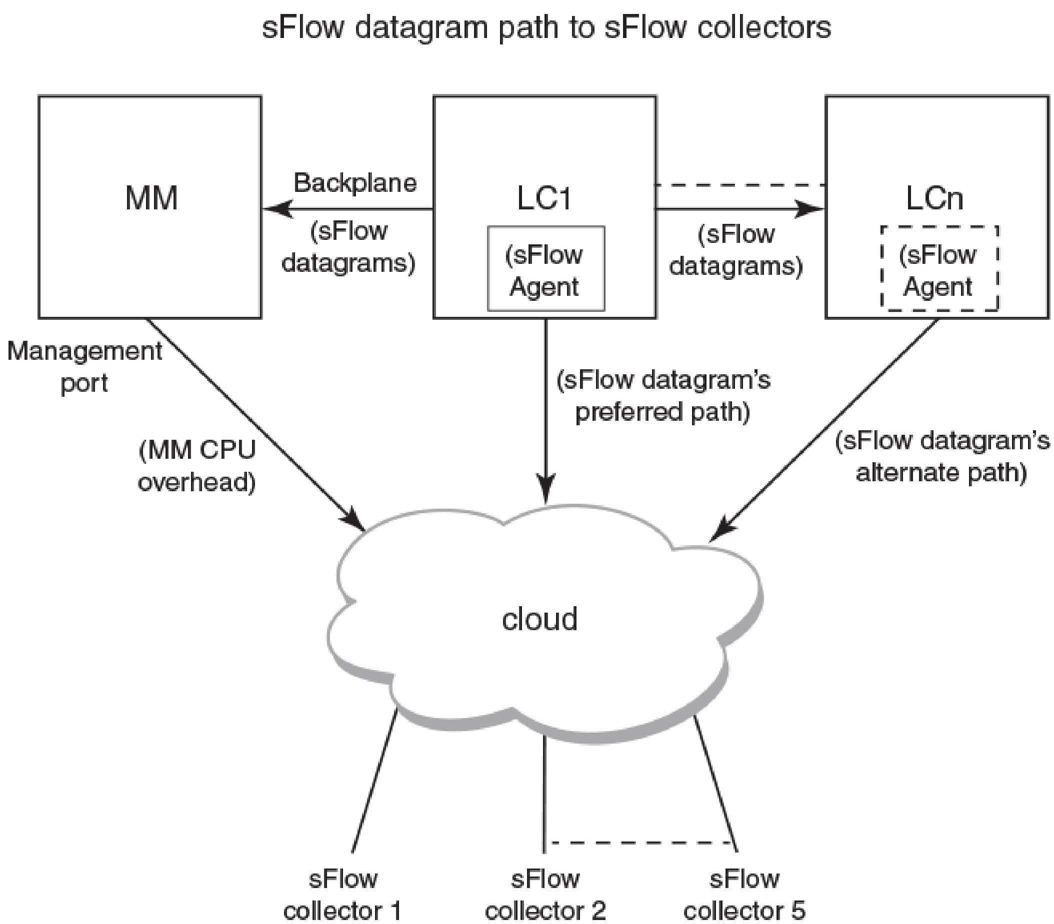
- User ACL based sflow
- VxLAN visibility sflow

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.

Feature support matrix for sFlow

The following table captures the sFlow feature support matrix for this release.

TABLE 6 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
Multi-sample grouping	Supported Grouping is decided by a timeout value (1 sec per RFC 3176) since the first sample was collected. It can combine both flow and counter samples in the same datagram. This increases the efficiency and scalability.
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 MPLS L2/3 VPN Endpoints	Supported
sFlow Support on MPLS Uplinks	Supported
sFlow support on VE interface	Supports only ingress policy.
sFlow support on VxLAN tunnels	Supported In addition to the VxLAN tunnel related information specified in the sFlow Data source flag and Input interface index fields, VxLAN extension headers are supported for Ingress packet sampled before encapsulation and Ingress packet sampled before decapsulation.

sFlow MPLS sampling support

The following table captures the sFlow MPLS sampling support matrix for this release. The first column indicates the type of MPLS configuration and the rest of the columns indicate the MPLS extension headers that are supported in sFlow sample at each node.

TABLE 7 sFlow support on MPLS

MPLS Configuration	LER Ingress	Transit Node	PHP Node	LER Egress
VLL/VPLS Local	Ext MPLS VC	NA	NA	NA
VLL/VPLS Outbound	Ext MPLS Tunnel Ext MPLS VC	Ext MPLS Data (stack depth = 2)	Ext MPLS Data (in label depth = 2) (out label = VC)	Ext MPLS Data (in label = VC, out label empty)
L3VPN	Ext MPLS Tunnel Ext MPLS VC	Ext MPLS Data (stack depth = 2)	Ext MPLS Data (in label depth = 2) (out label = VC)	Ext MPLS Data (in label = VC, out label empty)
IP over MPLS	Ext MPLS Tunnel	Ext MPLS Data (stack depth = 1)	Ext MPLS Data (in label depth = 1) (out label empty)	NA

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.

Configuring ACL based sFlow

Configuring ACL based sFlow involves the following.

- Create a standard or extended access-list.
- Add rules to the access-list with copy-sflow keyword.
- Bind the ACL to an interface.
- Monitor the ACL based sFlow per LC counters.
- Monitor the sflow sampled packets on sFlow collector.

Execute the following steps to configure ACL based sFlow.

1. Create an access list (standard or extended).
   - To create a standard access list:

   a) Execute the **mac access-list standard** command to create a standard MAC access-list **std-mac1** and add filters for the ACL based sFlow.

```
device(config)# mac access-list standard std-mac1
device(conf-macl-std)# permit 0.2020.0000 0.ffff.0000 copy-sflow
```

   b) Execute the **ip access-list standard** command to create a standard IPv4 access-list **std-vfour1** and add filters for ACL based sFlow.

```
device(config)# ip access-list standard std-vfour1
device(conf-ipacl-std)# permit 20.20.20.0 255.255.255.0 copy-sflow
```

   c) Execute the **ipv6 access-list standard** command to create a standard IPv6 access-list **std-vsix1** and add filters for ACL based sFlow.

```
device(config)# ipv6 access-list standard std-vsix1
device(conf-ip6acl-std)# permit host 10::10 copy-sflow
```

   - TO create an extended access list:

   a) Execute the **mac access-list extended** command to create an extended MAC access-list **ext-mac1** and add filters for ACL based sFlow.

```
device(config)# mac access-list extended ext-mac1
device(conf-macl-ext)# permit 0000.3030.0000 0000.ffff.0000 any copy-sflow
```

   b) Execute the **ip access-list extended** command to create an extended IPv4 access-list **ext-vfour1** and add filters for ACL based sFlow.

```
device(config)# ip access-list extended ext-vfour1
device(conf-ipacl-ext)# permit 30.30.30.0 255.255.255.0 any copy-sflow
```

   c) Execute the **ipv6 access-list extended** command to create an extended IPv6 access-list **ext-vsix1** and add filters for ACL based sFlow.

```
device(config)# ipv6 access-list extended ext-vsix1
device(conf-ip6acl-ext)# permit host 20::20 any copy-sflow
```

2. Bind the access list to an interface.
   - Execute the **interface ethernet** command to bind the extended MAC access-list **ext-mac1** to a physical interface.

```
device(config)# interface Ethernet 4/1
device(conf-if-eth-4/1)# mac access-group ext-mac1 in
```

   - Execute the **interface ethernet** command to bind the extended IPv4 access-list **ext-vfour1** to a physical interface.

```
device(config)# interface Ethernet 4/1
device(conf-if-eth-4/1)# ip access-group ext-vfour1 in
```

   - Execute the **interface ethernet** command to bind the extended IPv6 access-list **ext-vsix1** to a physical interface.

```
device(config)# interface Ethernet 1/4/1
device(conf-if-eth-1/4/1)# ipv6 access-group ext-vsix1 in
```

NOTE
ACL based sFlow uses the global sampling rate. The default value of global sampling rate is 2048. One packet out of every 2048 packets will be sampled. No check is be performed during ACL creation or ACL binding to validate the configuration of sFlow collector. If sFlow collector is not configured, the sampled packets are dropped at the CPU.

3. Execute the **show sflow** command to view the global sFlow configuration information and statistics, including the ACL based sFlow statistics.

```
device# show sflow
sFlow services are:                      enabled
Global default sampling rate:            32768 pkts
Global default counter polling interval: 1000 secs
sFlow Collector VRF:                     default-vrf
Rbridge-Id                           Collector server address
   Number of samples sent
----------------------------------------------------------------------------------------------------
----
         1                               10.120.75.1:6343                                      1609

ACL based samples collected (permit):     100
ACL based samples collected (deny)  :       0
```

4. Execute the **show sflow all** command to view global and per-port sFlow configuration information and statistics, including ACL based sFlow statistics.

```
device# show sflow all
sFlow services are:                       enabled
sFlow null0 sampling:                     disabled
Global default sampling rate:             32768 pkts
Global default counter polling interval: 1000 secs
sFlow Collector VRF:                      default-vrf
Rbridge-Id                            Collector server address                      Number of samples
sent
----------------------------------------------------------------------------------------------------
----
        1                             10.120.75.1:6343                                          1609

ACL based samples collected (permit):     100
ACL based samples collected (deny)  :       0


sFlow info for interface Ethernet 4/1
------------------------------------------------
Port based sflow services are:          enabled
Flow based sflow services are:          disabled
Configured sampling rate:               4096 pkts
Actual sampling rate:                   4096 pkts
Counter polling interval:               20 secs
Port backoffThreshold :                 96
Flow samples collected :                0
Counter samples collected :             10979

ACL based samples collected (permit) : 100
ACL based samples collected (deny)   : 50
```

Configuring sFlow on specific interfaces

Execute the following steps to configure sFlow on a specific interface.

1. Enter the configure terminal command to change to global configuration mode.

```
device # configure terminal
```

2. Enable sFlow forwarding on physical interfaces.

```
device (config)# interface ethernet 4/4
device (conf-if-eth-4/4)# sflow enable
```

3. Return to configuration mode using the **exit** command.

```
device (conf-if-eth-4/4)# exit
```

4. Configure other optional sflow configuration parameters.

```
device (config)# sflow source-interface ve 221
device (config)# sflow source-interface loopback 1
device (config)# sflow source-interface ethernet 4/4
```

NOTE
The interface configuration parameters override their global counterparts, for that interface. Following parameters can be configured globally or for individual interfaces.

```
device (config)# sflow polling-interval 233
deviec(conf-if-eth-4/4)# sflow polling-interval 233
<1-65535> Counter polling interval value. Use 0 to disable (default = 20)[234]
device (config)# sflow sample-rate 456
device(conf-if-eth-4/4)# sflow sample-rate 16000
<1-100000> Sampling rate value (default = 2048)[2048]
```

5. Execute any of the following commands to confirm the sFlow configuration status.

```
show sflow all
show sflow interface eth 1/46:2
show sflow linecard 1
show run sflow
```

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.

Configuration example

Global configuration

```
device(config)# sflow enable
2015/12/02-02:48:06, [SFLO-1001], 71, M1 | Active | DCE, INFO, Device, sFlow is
enabled globally.
device(config)# no sflow enable

2015/12/02-03:30:10, [SFLO-1001], 94, M1 | Active | DCE, INFO, Device, sFlow is
disabled globally.


device(config)# sflow sample-rate 4096

2015/12/02-03:12:35, [SFLO-1003], 82, M1 | Active | DCE, INFO, Device, Global sFlow sampling rate
is changed to 4096.

device(config)# no sflow sample-rate

2015/12/02-03:29:45, [SFLO-1003], 93, M1 | Active | DCE, INFO, Device, Global sFlow sampling rate
is changed to 2048.


device(config)# sflow polling-interval 30

2015/12/02-03:13:05, [SFLO-1004], 84, M1 | Active | DCE, INFO, Device, Global sFlow polling
interval is changed to 30.

device(config)# no sflow polling-interval

2015/12/02-03:29:26, [SFLO-1004], 92, M1 | Active | DCE, INFO, Device, Global sFlow polling
interval is changed to 20.


device(config)# sflow collector 172.22.108.57 6343

2016/03/18-05:07:18, [SFLO-1007], 680, M1 | Active | DCE, INFO, MMVM, 172.22.108.57 is
configured as sFlow collector.

device(config)# sflow collector 10.1.15.2 6343 use-vrf default-vrf

2016/03/18-05:07:40, [SFLO-1007], 681, M1 | Active | DCE, INFO, MMVM, 10.1.15.2 is
configured as sFlow collector.


device(config)# vrf red_vrf

device(config-vrf-red_vrf)# address-family ipv4 unicast
device(vrf-red_vrf-ipv4-unicast)# exit
device(config-vrf-red_vrf)# exit

device(config)# sflow collector 100.1.1.2 6343 use-vrf red_vrf
2016/03/18-05:08:41, [SFLO-1007], 682, M1 | Active | DCE, INFO, MMVM, 100.1.1.2 is
configured as sFlow collector.

device(config)# do show sflow

sFlow services are:                      disabled

sFlow null0 sampling:                    disabled

Global default sampling rate:            2048 pkts
Global default counter polling interval: 20 secs

Collector server address                        Vrf-Name     Sflow datagrams sent
----------------------------------------------------------------------------------

10.1.15.2:6343                               default-vrf                   0
```

```
100.1.1.2:6343                        red_vrf                        0

172.22.108.57:6343                     mgmt-vrf                      0


ACL based samples collected (permit):    0

ACL based samples collected (deny):      0

VxLAN Visibility samples collected:      0


device(config)# do show run sflow
sflow collector 10.1.15.2 6343 use-vrf default-vrf

sflow collector 100.1.1.2 6343 use-vrf red_vrf

sflow collector 172.22.108.57 6343 use-vrf mgmt-vrf device(config)#


device(config)# no sflow collector 172.22.108.57
2015/12/02-03:09:26, [SFLO-1007], 77, M1 | Active | DCE, INFO, Device, 172.22.108.57
is unconfigured as sFlow collector.

device(config)# no sflow collector 10.1.15.2 6343 use-vrf default-vrf

2015/12/02-03:09:26, [SFLO-1007], 77, M1 | Active | DCE, INFO, Device, 10.1.15.2 is
unconfigured as sFlow collector.

device(config)# no sflow collector 100.1.1.2 6343 use-vrf red_vrf

2015/12/02-03:09:26, [SFLO-1007], 77, M1 | Active | DCE, INFO, Device, 100.1.1.2 is
unconfigured as sFlow collector.
```

Interface configuration

```
device(config)# sflow source-interface eth 1/15
2015/12/02-03:01:12, [SFLO-1018], 76, M1 | Active | DCE, INFO, Device, sFlow SourceIP Interface is
changed to ethernet 1/15 (Eth1.15).
device(config)# no sflow source-interface
2015/12/02-03:28:50, [SFLO-1018], 91, M1 | Active | DCE, INFO, Device, sFlow SourceIP

Interface is changed to None (null) (None).
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
```