ADMINISTRATION GUIDE

Extreme Network OS Monitoring/RAS Administration Guide, 7.2.0

Supporting Network OS 7.2.0

53-1005144-02
10 July 2017

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Extreme 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.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, 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.

Extreme resources

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

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

Document feedback

Quality is our first concern at Extreme, 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:

- Use our short online feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/
- Email us at internalinfodev@extremenetworks.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 Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

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

- GTAC (Global Technical Assistance Center) for immediate support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal - Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

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

About This Document

What's new in this document

On October 30, 2017, Extreme Networks, Inc. acquired the data center networking business from Brocade Communications Systems, Inc. This document has been updated to remove or replace references to Brocade Communications, Inc. with Extreme Networks., Inc., as appropriate.

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 Extreme Networks, Inc. for Network OS, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Network OS:

- ExtremeSwitching VDX 2746
- ExtremeSwitching VDX 6740
  - ExtremeSwitching VDX 6740-48
  - ExtremeSwitching VDX 6740-64
- ExtremeSwitching VDX 6740T
  - ExtremeSwitching VDX 6740T-48
  - ExtremeSwitching VDX 6740T-64
  - ExtremeSwitching VDX 6740T-1G
- ExtremeSwitching VDX 6940-36Q
- ExtremeSwitching VDX 6940-144S
- ExtremeSwitching VDX 8770
  - ExtremeSwitching VDX 8770-4
  - ExtremeSwitching VDX 8770-8

To obtain information about a Network OS version other than this release, refer to the documentation specific to that version.

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.

The commands used for hardware threshold monitoring are configured in RBridge ID configuration mode to support fabric cluster and logical chassis cluster topologies.

System Resource Monitoring (SRM)

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

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

With the per-process memory monitoring service enabled, if the high memory usage threshold is crossed for any of the processes, 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.

If the system memory monitoring service is enabled, SRM generates raslog to notify that the system memory usage crossed the set threshold. If the per-process memory monitoring service is enabled, SRM generates a WARNING message if any of the processes consumes more memory. If usage further goes up, a CRITICAL message is generated. If the CPU utilization monitoring service is enabled, SRM generate raslog to notify that the CPU usage exceeded threshold of 90%.

This functionality is provided by the **resource-monitor** command. For more information on the command, please refer the *Network OS Command Reference*.

Configuring system resource monitoring

Execute the following steps to configure resource monitoring.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Issue the **rbridge-id** command to enter RBridge ID configuration mode.

   ```
   device(config)# rbridge-id 154
   ```

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

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

4. Issue the **resource-monitor memory** command to enable the system memory monitoring and generate raslog when the memory usage exceeds threshold value.

   ```
   device(config-rbridge-id-154)# resource-monitor memory enable action raslog threshold 150
   ```

5. Issue the **resource-monitor process memory** command to enable the per-process memory monitoring and generate alarm or raslog when the usage exceeds alarms threshold or critical threshold respectively.

   ```
   device(config-rbridge-id-154)# resource-monitor process memory  enable alarm 550 critical 650
   ```

6. (Optional) Issue the how running-configuration command to view the resource monitoring running configuration.

   ```
   device# show running-config rbridge-id resource-monitor
   rbridge-id 154
    resource-monitor cpu enable
    resource-monitor memory enable threshold 150 action raslog
    resource-monitor process memory enable alarm 550 critical 650
   !
   device#
   ```

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

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.

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.

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**. When memory usage exceeds or falls below this limit, a RASLog INFO message is sent.

poll Specifies the polling interval in seconds. Valid values range from 0 through 3600.

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

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

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

TABLE 1 Default values for CPU and memory threshold monitoring

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

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. Use the **rbridge-id** command to enter RBridge ID configuration mode.

   ```
   device(config)# rbridge-id 154
   ```

3. 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-rbridge-id-154)# threshold-monitor memory actions none high-limit 60 low-limit 40
   ```

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

   ```
   device(config-rbridge-id-154)# threshold-monitor cpu actions raslog limit 65 poll 60 retry 10
   ```

The following example sets hardware monitoring thresholds for memory and cpu-usage.

```
device# configure terminal
device(config)# rbridge-id 154
device(config-rbridge-id-154)# threshold-monitor memory actions none high-limit 60 low-limit 40
device(config-rbridge-id-154)# threshold-monitor cpu actions raslog limit 65 poll 60 retry 10
```

Viewing threshold status

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

```
switch# show running-config rbridge-id rbridge_id 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.

```
switch# 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 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.

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
```

Viewing the area-wise optical monitoring current status

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

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

Tunable SFP+ (T-SFP+) optics

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

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

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

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

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

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

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

Configuring optical monitoring thresholds and alerts

The following is an example of configuring SFP monitoring.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter **rbridge-id** *rbridge-id#* to change to RBridge ID configuration mode.

   ```
   device(config)# rbridge-id 154
   switch(config-rbridge-id-154)#
   ```

3. Enter **threshold-monitor sfp** and create a custom policy.

   ```
   device(config-rbridge-id-154)# threshold-monitor sfp policy custom type 1glr area temperature alert
   above highthresh-action raslog email
   ```

4. Apply the policy.

   ```
   device(config-rbridge-id-154)# threshold-monitor sfp apply mypolicy
   ```

SFP thresholds

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

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

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

TABLE 3 Factory thresholds for SFP types and monitoring areas

SfpType	Area	Default Value	
1 GSR	Temperature (C)	100	-40
	Voltage (mV)	3600	3000
	RXP (µW)	1122	8
	TXP (µW)	1000	60
	Current (mA)	12	2
1 GLR	Temperature (C)	90	-45
	Voltage (mV)	3700	2900
	RXP (µW)	501	6
	TXP (µW)	794	71
	Current (m)	45	1
10 GSR	Temperature (C)	90	-5
	Voltage (mVolt)	3600	3000
	RXP (µW)	1000	32
	TXP (µW)	794	251
	Current (mA)	11	4
10 GLR	Temperature (C)	88	-5
	Voltage (mV)	3600	2970
	RXP (µW)	1995	16
	TXP (µW)	1585	158
	Current (mA)	85	15
10 GUSR	Temperature (C)	100	-5
	Voltage (mV)	3600	2970
	RXP (µW)	2000	32
	TXP (µW)	2000	126
	Current (mA)	11	3
QSFP	Temperature (C)	75	-5
	Voltage (mV)	3600	2970
	RXP (µW)	1995	40
	TXP (µW)	0	0
	Current (mA)	10	1

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.

Cyclic redundancy check (CRC)

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

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

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

Port CRC supports following actions:

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

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

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

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

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

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

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

```
device# show interface ethernet 3/4
Ethernet 3/4 is port-CRC down, line protocol is down (port-crc down)
Hardware is Ethernet, address is 00e0.0c76.79e8
    Current address is 00e0.0c76.79e8
Pluggable media not present
Interface index (ifindex) is 415367190
MTU 1548 bytes
10G Interface
```

```
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Last clearing of show interface counters: 13:19:17
Queueing strategy: fifo
Receive Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Bro
```

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

```
device# show ip interface brief

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

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

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

Diagnostic Port

Enhanced support for 32G QSFPs

In Fabric OS 8.1.0a and later, support is provided for electrical and optical loopback tests on 32G-QSFPs that support E_WRAP and O_WRAP.

Not all QSFPs currently available support E_WRAP and O_WRAP. Generally, E_WRAP must be set on both ends of the link, and O_WRAP must be set on the remote end. ISL-to-ISL connections are supported but ICL -to- ICL connections are not. (This support is available on breakout cables.) Both switches must have QSFPs that support E_WRAP and O_WRAP. The following are supported connections:

- 32G QSFP ISL < -- > 32G QSFP ISL
- 32G QSFP ISL < -- > 32G SFP ISL
- 32G QSFP ICL < -- > 32G QSFP ICL

Limitations

The following QSFPs do not support this feature:

- JAF1: 32G Finisar version 1
- JAF2: 32G Finisar version 2
- JAA1: 32G Avago version 1
- AD1: 32G Avago with early hardware upgraded to JAA2 firmware
- JAA2: 32G Avago version 2
- The earlier versions of the 32G QSFP, having serials number starting with “ZTA” and next 5-digit number less than “11547” (for example, ZTA11516000000K, ZTA11517000001F)

In addition, if one end of the link has older 16G- or 32G-QSFPs or QSFPs that do not support E_WRAP or O_WRAP, and the other end supports this feature, electrical loopback test will run on the end which supports the feature. Optical loopback test is not supported.

ATTENTION

The following restrictions apply to both 32G/16G breakout QSFP and 32G fixed-speed QSFPs. These restrictions are not applicable if these QSFPs are in ICL ports.

- Fabric OS enforces the same static D_Port configuration for all channels in the QSFP ports, for both 32G/16G breakout QSFPs and 32G fixed-speed QSFPs.
- Fabric OS blocks dynamic and skips on-demand D_Port tests for 32G/16G breakout QSFPs and 32G fixed-speed QSFPs.
- D_Port tests will not start if the channels of a 32G QSFP are connected to different logical switches.

A warning message appears when the static D_Port configuration for QSFPs is changed. D_Ports test will not start if the channels of 32G QSPF are connected to different logical switches.

With these restrictions, an Emulex HBA cannot run on-demand D_Port tests. For an Emulex HBA, you must configure a static D_Port on the switch side and initiate D_Port tests from the Emulex HBA side.

Example output

Prior to Fabric OS 8.1.0, electrical and optical D_Port tests were displayed as "SKIPPED" as they were unsupported, as in the following example output.

```
switch> portdporttest --show 55
D-Port Information:
===================
Port:                55
Remote WWNN:            10:00:00:27:f8:f0:26:38
Remote port index:        55
Mode:                Manual
No. of test frames:        1 Million
Test frame size:        1024 Bytes
FEC (enabled/option/active):    Yes/No/Yes
CR (enabled/option/active):    Yes/No/No
Start time:            Mon Apr 18 09:57:43 2016
End time:            Mon Apr 18 09:57:50 2016
Status:                PASSED
================================================================================
Test             Start time    Result        EST(HH:MM:SS)    Comments
================================================================================
Electrical loopback    --------    SKIPPED        --------    No SFP or chip support
Optical loopback       09:57:44    SKIPPED        --------    ----------
Link traffic test      09:57:46    PASSED         --------    ----------
================================================================================
Roundtrip link latency:        1116 nano-seconds
Approximate cable distance:    unknown
Buffers required:            1 (for 2112 byte frames at 32Gbps speed)
Egress power:                            Tx: Not Avail, Rx: -1.6 dBm.
Ingress power:                        Rx: -0.5 dBm, Tx: -23.6dBm, Diff: 0.0 dBm (No Loss)62:FID128:root>
```

With current support, results are displayed as either "PASSED" or "FAILED" as in the following example output.

```
device:FID128:root> portdporttest --show 55
D-Port Information:
===================
Port:                55
Remote WWNN:            10:00:00:27:f8:f0:26:30
Remote port index:        55
Mode:                Automatic
No. of test frames:        1 Million
Test frame size:        1024 Bytes
FEC (enabled/option/active):    Yes/No/Yes
CR (enabled/option/active):    Yes/No/No
Start time:            Mon Apr 18 09:43:42 2016
End time:            Mon Apr 18 09:43:51 2016
Status:                PASSED
=============================================================================
Test             Start time    Result        EST(HH:MM:SS)    Comments
=============================================================================
Electrical loopback    09:43:42    PASSED        --------    ----------
Optical loopback       09:43:44    PASSED        --------    ----------
Link traffic test      09:43:47    PASSED     --------    ----------
=============================================================================
Roundtrip link latency:        1113 nano-seconds
Approximate cable distance:    unknown
Buffers required:            1 (for 2112 byte frames at 32Gbps speed)
Egress power:                            Tx: -18.7dBm, Rx: -0.5 dBm, Diff: 0.0 dBm (No Loss)
Ingress power:                        Rx: -1.6 dBm, Tx: Not Avail.
62:FID128:root>
```

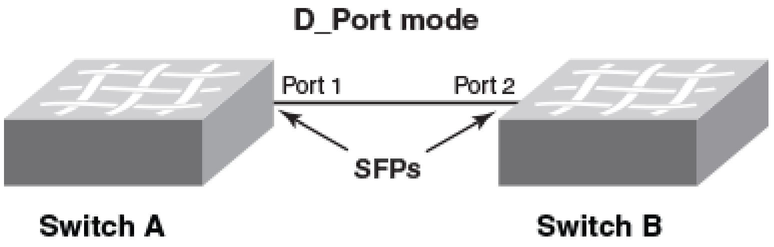
Understanding D_Port

A port in D_Port mode does not carry any user traffic, and is designed to run only specific diagnostics tests for identifying link-level faults or failures.

The following figure illustrates an example D_Port connection between a pair of switches through SFP transceivers (port assignments will vary).

> NOTE
> D_Port functionality is supported only on TRILL-capable links between two Network OS switches.

FIGURE 1 Example of a basic D_Port connection between switches



To bring up a port in D_Port mode, follow these basic steps:

1. Disable the ISL capability on the ports. (**no fabric isl enable**)
2. Enable D_Port functionality on both ends of the link. (**fabric dport mode static**)
3. Enable the ISL capability on the ports. (**fabric isl enable**)

> NOTE
> Detailed configuration examples are presented later in this chapter.

Once the ports are configured and enabled as D_Ports, a link traffic test is executed for 10-Gbps SFPs, 10*4-Gbps QSFPs, 40-Gbps SFPs, or 100-Gbps SFPs.

The user configures the desired ports on either end, or both ends, of the connection. (The default D_Port mode of a port is dynamic mode. If the user configures one end as D_Port static mode, then the other end behaves as a D_Port. Alternatively, the user can configure both ends as D_Port static mode.) Once both sides are configured, a basic test suite is initiated automatically when the link comes online. After the automatic test is complete, the user can view results through the CLI or a GUI and rectify issues (if any) that are reported. The user can also start (and restart) the test manually to verify the link.

General limitations and considerations for D_Port tests

Consider the following issues when running D_Port tests:

- Testing is supported in management cluster and logical chassis cluster modes.
- D_Port testing is not supported between Network OS Fibre Channel ports, including between an Access Gateway to Fabric OS connections and between ISLs and Fabric OS EX_Port connections.
- The link to be tested must be marginally functional and able to carry a minimal number of frames before it can become a D_Port link.
- D_Port testing is useful for diagnosing marginal faults only. A complete failure of any component cannot be detected.
- Switches must be configured with the same VCS ID and the same default FCoE VLAN.
- Tests can be run within a cluster, as well as in a noncluster configuration. The switches are not required to be in the same cluster. Testing does not disrupt the cluster or fabric.
  - Within a cluster, disable the ISL (it must not be the only one if you want the cluster to stay up. Then set one or both sides to static mode and reenable the ISL. The test runs automatically.
  - In a noncluster configuration, no special configuration is required. Set the external switch to static mode to run tests on new ports in a cluster without disruption.
- You can configure multiple ports in parallel, in which case the tests are serialized. Keep in mind that the number of parallel ports and frame tests will affect the test time accordingly.
- Edge ports are not supported.
- Optical and electrical loopback tests are not supported for TRILL ISLs. Instead, Brocade spinFab creates a loopback route on both ends of the link, millions of frames are looped, and statistics are gathered.
- TRILL ISL ASIC limitations apply to supported tests.
- Before downgrading to a release that does not support D_Port, the port type must be cleared of the D_Port configuration.
- D_Port configuration is not supported on mezzanine cards.
- D_Ports do not support a loop topology.
- D_Port testing is not supported on adapter ports configured in CNA mode.
- Toggling the port on either side of the link restarts the test.
- When a large number of D_Ports are configured, the test is run on one port per blade at a time, and other ports wait until the test is completed. No test begins until the fabric is stable.

High Availability limitations and considerations for D_Ports

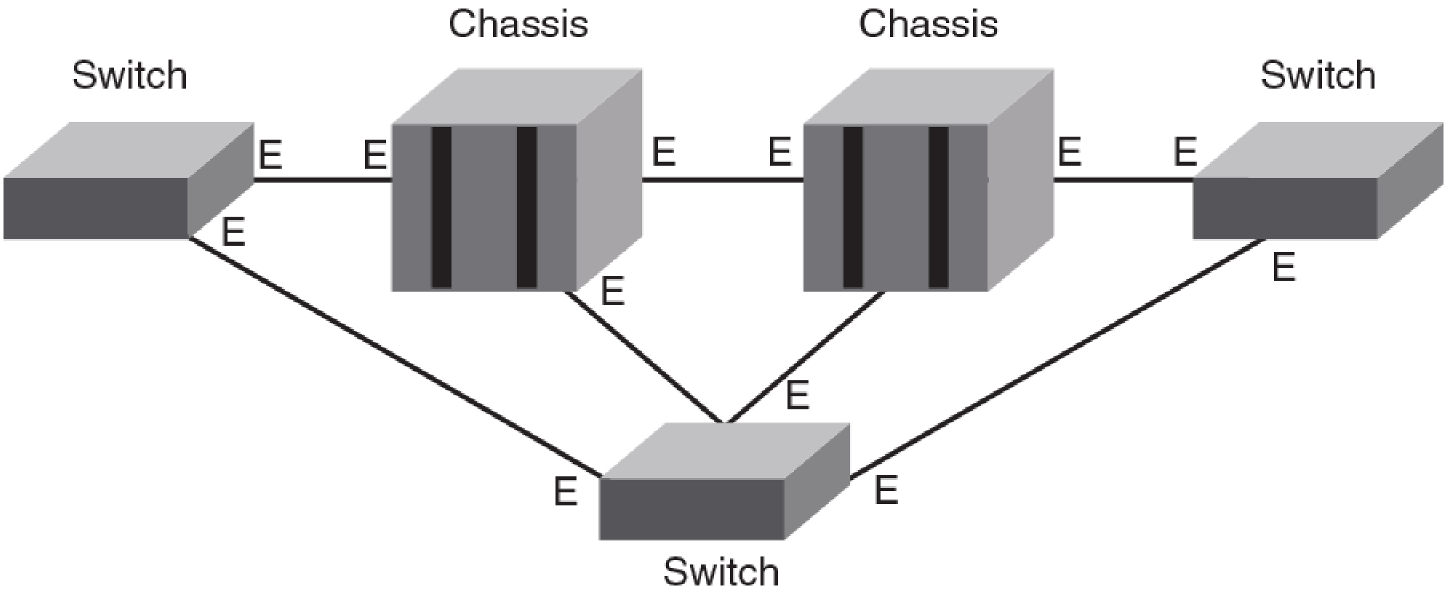
Consider the following High Availability (HA) limitations and considerations when using D_Ports:

- There is no HA support for D_Port test options and results. Any information from a previous test is lost following a failover or reboot.
- During an HA failover reboot on one side of the link, the link is reinitialized and may restart the test. However, the test cannot proceed if the remote port is not ready to proceed further (the remote port may already be done with the D_Port test and in the final state). In such a case, the test will eventually fail with a “Remote port not ready” message. Restarting the test from either side will recover the port.

Topology 1: ISLs

The following figure illustrates inter-switch links (ISLs) that connect multiple switches through a pair of chassis. The letter E represents E_Ports to be configured as D_Ports.

FIGURE 2 ISLs connecting multiple switches and chassis



Note the following:

- Only static-static and static-dynamic D_Port modes are supported on the ISLs.

Using D_Port in static-static mode between switches

This section illustrates the configuration of static-static mode on ISLs for the illustrated topology.

Enabling D_Port in static mode

Use this procedure to configure a basic, automatic D_Port diagnostics session in static mode between two switches. The summary steps are as follows:

1. Disable ISL functionality on the ports.
2. Configure D_Port static mode on both ends of the link.
3. Enable ISL functionality on the ports.

ATTENTION
The automatic test might fail if you do not follow the sequence of steps exactly.

NOTE
"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested. Switch A and Switch B can the same platform or different platforms supporting an end-to-end D_Port connection.

The detailed steps are as follows:

1. Disable Port 1 on Switch A.

   NOTE
   This example uses TenGigabitEthernet ports.

   ```
   device# config
   device(config)# int te 52/0/35
   device(conf-if-te-52/0/35)# no fabric isl enable
   device(conf-if-te-52/0/35)#
   ```

2. Configure Port 1 on Switch A as a D_Port in static mode.

   ```
   device(conf-if-te-52/0/35)# fabric dport mode static
   device(conf-if-te-52/0/35)#
   ```

3. Repeat Step 1 and Step 2 for the corresponding port (in this example, Port 2) on Switch B.

   ```
   device# config
   device(config)# int te 52/0/35
   device(conf-if-te-52/0/35)# no fabric isl enable
   device(conf-if-te-52/0/35)# fabric dport mode static
   ```

4. Re-enable Port 1 on Switch A.

   ```
   device(conf-if-te-52/0/35)# fabric isl enable
   device(conf-if-te-52/0/35)#
   ```

5. Re-enable Port 2 on Switch B.

   ```
   device(conf-if-te-52/0/35)# fabric isl enable
   device(conf-if-te-52/0/35)#
   ```

   The basic test suite starts as soon as both ports are enabled and ready to perform the test.

   NOTE
   For the details of using the available nondefault test options, see the **diag dport-test** command.

6. To confirm D_Port configuration on a port, as reflected in the running configuration, use the following command:

   ```
   device(config)#  sh run int te 1/2/8
   interface TenGigabitEthernet 1/2/8
   fabric isl enable
   fabric trunk enable
   fabric dport mode static
   no shutdown
   ```

7. While the test is running, you can enter a variety of **show** commands to confirm the D_Port configuration and view test results on an interface. See "Using D_Port show commands" at the end of this chapter.

   To view D_Port status and test results for an interface:

```
device# show dport-test interface Tengigabitethernet 238/0/96
D-Port Information:
===================
Interface Name:                         Te 238/0/96
Index:                                  239
Remote Interface Name:                  Te 24/0/2
Remote Index:                           145
Remote WWNN:                            10:00:00:05:33:e7:f0:d0
Mode:                                   Automatic
No. of test frames:                     1 Million
Test frame size:                        1024 Bytes
Start time:                             Tue Feb  2 14:01:45 2016
End time:                               Tue Feb  2 14:02:27 2016
Status:                                 PASSED
===============================================================================================
Test                     Start time      Result          EST(HH:MM:SS)   Comments
===============================================================================================
Link traffic test        14:02:18        PASSED          --------        ----------
===============================================================================================
```

Disabling D_Port in static mode

Use this procedure to disable a D_Port diagnostics session in static mode, as configured in "Enabling D_Port in static mode."

NOTE
"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

1. Disable Port 1 on Switch A.

   NOTE
   This example uses TenGigabitEthernet ports.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)#
```

2. Disable the D_Port functionality in static mode on Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric dport mode none
device(conf-if-te-52/0/35)#
```

3. Repeat Steps 1 and Step 2 for Port 2 on Switch B.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)# fabric dport mode none
```

4. Reenable Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

5. Reenable Port 2 on Switch B.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

Disabling D_Port globally

You can prevent D_Port testing from running regardless of the configuration at the other end of the link.

1. Enter interface subtype configuration mode.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)#
```

2. Enter the **fabric dport mode none** command.

```
device(conf-if-te-52/0/35)# fabric dport mode none
device(conf-if-te-52/0/35)#
```

Using D_Port in dynamic mode

Enabling dynamic D_Port switch-wide configuration forces the ports on that switch or chassis to respond to D_Port requests from the other end of the connection. It basically responds to a remote port request to change its mode to D_Port mode, and run diagnostic tests automatically. For more information on enabling dynamic D_Port mode for all ports in a switch or chassis, refer to "D_Port configuration mode and testing" in this chapter.

Enabling D_Port in dynamic mode

Use this procedure to configure a basic D_Port diagnostics session in dynamic mode between two switches. The summary steps are as follows:

1. Disable the ports on both ends of the link.
2. Configure D_Port dynamic mode on Switch A.
3. Configure D_Port static mode on Switch B.
4. Enable the ports on both ends of the link.

ATTENTION
The automatic test might fail if you do not follow the sequence of steps exactly. You must also disable dynamic mode on a port if you want that port never to become a D_Port.

NOTE
"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

The detailed steps are as follows:

1. Disable Port 1 on Switch A.

   NOTE
   This example uses TenGigabitEthernet ports.

   ```
   device# config
   device(config)# int te 52/0/35
   device(conf-if-te-52/0/35)# no fabric isl enable
   device(conf-if-te-52/0/35)#
   ```

2. Configure Port 1 on Switch A as a D_Port in dynamic mode.

   ```
   device(conf-if-te-52/0/35)# fabric dport mode dynamic
   device(conf-if-te-52/0/35)#
   ```

3. Repeat Step 1 and Step 2 for the corresponding port in static mode (in this example, Port 2) on Switch B.

   ```
   device# config
   device(config)# int te 52/0/35
   device(conf-if-te-52/0/35)# no fabric isl enable
   device(conf-if-te-52/0/35)# fabric dport mode static
   ```

4. Re-enable Port 1 on Switch A.

   ```
   device(conf-if-te-52/0/35)# fabric isl enable
   device(conf-if-te-52/0/35)#
   ```

5. Re-enable Port 2 on Switch B.

   ```
   device(conf-if-te-52/0/35)# fabric isl enable
   device(conf-if-te-52/0/35)#
   ```

   The basic test suite starts as soon as both ports are enabled and ready to perform the test.

6. While the test is running, enter the following **show** command to view test results. The following test is successful.

7. To display a summary of the D_Port, use the following command.

Disabling D_Port in dynamic mode

Use this procedure to disable a D_Port diagnostics session in dynamic mode, as configured in "Enabling D_Port in dynamic mode."

NOTE
"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

ATTENTION

You must also disable dynamic mode on a port if you want that port never to become a D_Port.

1. Disable Port 1 on Switch A.

   NOTE

   This example uses TenGigabitEthernet ports.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)#
```

2. Disable the D_Port functionality in dynamic mode on Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric dport mode none
device(conf-if-te-52/0/35)#
```

3. Repeat Steps 1 and Step 2 for Port 2 on Switch B.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)# fabric dport mode none
```

4. Reenable Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

5. Reenable Port 2 on Switch B.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

Support for audit logs

In previous releases, log messages were not generated when a port was either configured or unconfigured as a D_Port.

The **switchShow** command was the only option available to verify whether a port was configured as a D_Port or not. With Fabric OS 8.1.0, the following log messages are provided.

NOTE

The following messages are supported only for static D_Port configurations.

This example log message is generated when a port is configured as a D_Port.

```
624 AUDIT, 2016/04/21-10:36:06 (UTC), [FABR-1075], INFO, RAS, admin/admin/172.26.3.151/telnet/CLI,
ad_0/Dport_DCX/FID 128,, Port is configured as D_port.
```

This example log message is generated when a port is unconfigured as a D_Port.

```
625 AUDIT, 2016/04/21-10:36:06 (UTC), [FABR-1075], INFO, RAS, admin/admin/172.26.3.151/telnet/CLI,
ad_0/Dport_DCX/FID 128,, Port is not configured as D_port.
```

Using D_Port show commands

This section presents a variety of options for viewing the results of D_Port testing.

The global **show running config interface** command shows the status of the D_Port test confiiguration on the configured port.

```
device# show running-config interface TenGigabitEthernet 52/0/35
interface TenGigabitEthernet 52/0/35
fabric isl enable
fabric trunk enable
fabric dport mode none
no shutdown
```

Use the above command in interface subtype configuration mode to see the same results.

```
device(conf-if-te-52/0/35)# do show running-config interface TenGigabitEthernet 52/0/35
interface TenGigabitEthernet 52/0/35
fabric isl enable
fabric trunk enable
fabric dport mode none
no shutdown
```

Use the **show dport-test interface** command to display basic test results for a specified interface.

```
show dport-test interface Tengigabitethernet 56/0/1
D-Port Information:
===================
Interface Name:                         Te 56/0/1
Index:                                  64
Remote Interface Name:                  Te 60/4/1
Remote Index:                           12
Remote WWNN:                            10:00:00:27:f8:1e:aa:48
Mode:                                   Automatic
No. of test frames:                     1 Million
Test frame size:                        1024 Bytes
Start time:                             Tue Feb  2 04:44:33 2016
End time:                               Tue Feb  2 04:44:47 2016
Status:                                 PASSED
=================================================================================
Test                    Start time      Result          EST(HH:MM:SS)   Comments
=================================================================================
Link traffic test       04:44:36        PASSED          --------        ---------
=================================================================================
```

Use the **show dport-test interface detail** command to display test results for the interface, as well as frame statistics for the port under test and any detailed errors.

NOTE

Statistics are cleared before a new test is started. The log is empty for a successful test.

```
device# show dport-test interface Tengigabitethernet 56/0/1 detail
D-Port Information:
===================
Interface Name:                         Te 56/0/1
Index:                                  64
Remote Interface Name:                  Te 60/4/1
Remote Index:                           12
Remote WWNN:                            10:00:00:27:f8:1e:aa:48
Mode:                                   Automatic
No. of test frames:                     1 Million
Test frame size:                        1024 Bytes
Start time:                             Tue Feb  2 04:44:33 2016
End time:                               Tue Feb  2 04:44:47 2016
Status:                                 PASSED
================================================================================+
Test                    Start time      Result          EST(HH:MM:SS)   Comments
=================================================================================
Link traffic test       04:44:36        PASSED          --------        ---------
```

```
=================================================================================
D-Port statistics:
=================================================================================
                                   RX                              TX
             Packets         3299499                         3300600
               Bytes      3602996140                      3603243530
            Unicasts         3299442                         3300533
          Multicasts              57                              67
          Broadcasts               0                               0
              Errors               0                               0
            Discards               0                               0
            Overruns               0      Underruns                0
               Runts               0
             Jabbers               0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts              46
  Over 127-byte pkts              10
  Over 255-byte pkts               1
  Over 511-byte pkts               1
 Over 1023-byte pkts         3299441
 Over 1518-byte pkts               0
           Mbits/Sec        0.000000                        0.000000
          Packet/Sec               0                               0
           Line-rate           0.00%                           0.00%

==================================================================================
Spinfab Log:
==================================================================================
Logs Unavailable
```

Use the **show dport-test rbridge-id** command to display summary test results for all D_Ports in a specified RBridge.

```
device# show dporttest rbridge-id 56

RBridge-Id : 56
==================================================================================
Index   Interface       State           D-Port Mode             Test Result
==================================================================================
64      Te 56/0/1       ONLINE          Static                  PASSED
87      Te 56/0/24      ONLINE          Static                  PASSED
==================================================================================
```

NOTE

The **rbridge-id all** option is not supported.

Use the **show dport-test all** command to display test results for all D_Ports in the fabric.

```
device# show dport-test all

RBridge-Id : 60
==================================================================================
Index   Interface       State           D-Port Mode             Test Result
==================================================================================
12      Te 60/4/1       ONLINE          Dynamic                 PASSED
==================================================================================

RBridge-Id : 55
==================================================================================
Index   Interface       State           D-Port Mode             Test Result
==================================================================================
86      Te 55/0/23      ONLINE          Dynamic                 PASSED
==================================================================================

RBridge-Id : 56
==================================================================================
Index   Interface       State           D-Port Mode             Test Result
==================================================================================
64      Te 56/0/1       ONLINE          Static                  PASSED
```

```
87      Te 56/0/24      ONLINE          Static                  PASSED
==================================================================================
```

Port Mirroring

Port mirroring overview

Port mirroring, known as Switched Port Analyzer (SPAN) is used on a network switch to send a copy of network packets seen on one switch port to a network monitoring connection on another switch port.

Unlike a hub which broadcasts any incoming traffic to all ports, a switch acts more intelligently and forwards traffic accordingly. If the user is interested in listening or snooping on traffic that passes through a particular port, port mirroring is necessary to artificially copy the packets to a port connected to the analyzer.

Usually, SPAN traffic is limited to incoming or outgoing packets, but Network OS 4.0.0 and later allows bidirectional traffic monitoring on the source port.

SPAN in logical chassis cluster

SPAN in logical chassis cluster supports mirroring of a source port to a destination port lying on a different switch in the cluster. SPAN in logical chassis cluster is configured in the same manner, with the exception of the **source** command.

RSPAN

Remote SPAN, or RSPAN, extends SPAN by enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN and then forwarded over trunk ports that are carrying the RSPAN VLAN to any RSPAN destination sessions monitoring the RSPAN VLAN.

> NOTE
> RSPAN is supported only on Extreme VDX 8770, VDX 6740, and VDX 6940 series platforms.

RSPAN consists of an RSPAN source interface and an RSPAN VLAN. The configured source port is mirrored to the RSPAN VLAN and the ports that are members of this VLAN receive the mirrored traffic.

All participating switches must be trunk-connected at Layer 2, and the remote VLAN must be configured on all the switches participating in the RSPAN session.

SPAN guidelines and limitations

Consider the following topics when configuring SPAN.

Standard SPAN guidelines and limitations

The following table lists the number of SPAN sessions with and without a shared destination port, as well as the number of SPAN sessions for both fabric-wide and VCS SPAN, with no sharing of the destination port.

NOTE
A SPAN session consists of either a single egress port, a single ingress port, or both.

We recommend that you be aware of the following additional standard guidelines for and limitations of SPAN connections:

- If there is congestion at the ingress span queue resulting from bandwidth-related back pressure at the ISL, the SPAN mirrored packets will be dropped and traffic will be lost.
- FCoE mirroring is not supported.
- For the traffic flowing across the switch, if the source port is in unknown mode (the node is in Layer 2 or Layer 3), then the untagged packets are dropped.
- The mirror port should not be configured to carry normal traffic.
- A port cannot be made a destination port for bidirectional mirroring if a different port supported by that ASIC is already configured as destination port for any type of mirroring.
- If a port is configured as a destination port for bidirectional mirroring, no other port supported by that ASIC can be made a destination port for any type of mirroring.
- The destination mirror port can handle from 1 to 40 Gbps (line rate) worth of mirror traffic, depending on the capability of the destination port. If multiple ports, or both flows on the same port, are mirrored to the same destination mirror port, then only the destination port's capacity worth of mirror traffic is mirrored and the remaining traffic is ignored.
- If the source port receives burst traffic and the destination mirror port cannot handle all the bursts, some of the burst traffic is not mirrored.
- Mirroring of LAG or port-channel interfaces is not supported, but LAG members can be mirrored.
- TRILL ports cannot be designated as a destination port.
- TRILL ports can be a source port, but mirroring is restricted to the port local to the source node ports.
- Ethernet Pause frames are not mirrored.
- Mirroring of trunk port is not supported, although the ASIC supports the mirroring of a trunk. To mirror a trunk, you must individually enable mirroring on all member ports.
- The multicast and broadcast statistics are correctly updated on TX ports for mirrored traffic.
- All commands except for **shutdown** and **no shutdown** are blocked on a destination mirror port.
- The interface counters are cleared when a port is successfully designated as a destination mirror port.
- The **show interface** command hides the Receive Statistics and Rate Info (Input) information for a destination mirror port.
- The MTU of a port should be set to the default value of 2500 bytes before it is made a destination mirror port. When the port is successfully designated as the destination mirror, the MTU of that port is automatically set to the maximum value of 9216 bytes. When the port becomes a non-destination mirror, the MTU is restored to the default value.
- Port mirroring is supported on any physical front-end user-configurable port. The source port can be part of a LAG, VLAG, VLAN, or any other user configuration
- A maximum of 512 mirror sessions are supported. A mirror session consists of either a single egress port, a single ingress port, or both.

ATTENTION
If you see egress traffic, you must change the TCAM profile (by means of the **hardware-profile** command) to "IPV4-V6-QOS".

NOTE
Remote Span (RSPAN) is not supported on this platform.

RSPAN guidelines and limitations

The following configurations and restrictions for RSPAN should be kept in mind.

Basic considerations

The following table lists the number of RSPAN sessions with and without a shared destination port, as well as the number of SPAN sessions for both fabric-wide and VCS SPAN, with no sharing of the destination port.

TABLE 4 Number of RSPAN sessions supported under various conditions

Extreme platform	Number of sessions without shared destination port	Number of sessions with shared destination port	Number of sessions, for both fabric-wide and VCS SPAN, without shared destination port
VDX 6740/6790 series	7	24	7 per box, 512 per VCS
VDX 8770 series	8 per port group, 48 per line card, 48 per chassis	No sharing needed (8 ports support 8 sessions)	48 per box, 512 per VCS

We recommend that you be aware of the following additional standard guidelines for and limitations of RSPAN connections:

- All participating switches must be connected by Layer 2 trunks.
- Inter-Switch Link (ISL) mirroring is not supported on RSPAN.
- The source and destination ports cannot both be TRILL (ISL) ports.
- RSPAN supports multi-hop.
- If the source port is not Layer 2 and untagged traffic is mirrored, it will be dropped for RSPAN because untagged and unclassified traffic is dropped on an ISL trunk.
- On the Extreme VDX 6740 series platforms, if source port is in unknown mode, that is neither Layer 2 nor Layer 3, the packets are dropped and are not mirrored.
- Ethernet Pause frames are not mirrored.

ATTENTION
With bidirectional flow-based RSPAN, where policy maps with IP ACLs are used, the TCAM profiles need to be changed (by means of the **hardware-profile** command) if TCAM resources are not allocated for "IPv4 ACL Based QoS Policy Entries (Egress)" and "IPv6 ACL Based QoS Policy Entries (Egress)". Note the highlighted lines in the following output of the **show hardware-profile current** command.

```
device# show hardware-profile current

rbridge-id: 24                 switch type: BR-VDX6740

                       current TCAM profile:    DEFAULT
________________________________________________________
                        L2 Path Select FCoE:    512
 MAC ACL Based QoS Policy Entries (Ingress):    512
                  L2 Path Select FCoE Zones:    0
         MAC Security ACL Entries (Ingress):    512
        MAC Policy Based forwarding entries:    0
    L2 Multicast No Flood Entries (Ingress):    0
IPV4 ACL Based QoS Policy Entries (Ingress):    512
           IPV4 Multicast Entries (Ingress):    1024
IPV4 Policy Based Routing Entries (Ingress):    512
        IPV4 Security ACL Entries (Ingress):    512
                        L3 Path Select FCoE:    512
IPV6 Policy Based Routing Entries (Ingress):    0
IPV6 ACL Based QoS Policy Entries (Ingress):    0
           IPV6 Multicast Entries (Ingress):    0
        IPV6 Security ACL Entries (Ingress):    512
                    IPV4 Forwarding Entries:    4096
                            L2 Forward FCoE:    2048
                    IPV6 Forwarding Entries:    1024
          MAC Security ACL Entries (Egress):    128
  MAC ACL Based QoS Policy Entries (Egress):    128
         IPV4 Security ACL Entries (Egress):    128
 IPV4 ACL Based QoS Policy Entries (Egress):    0
         IPV6 Security ACL Entries (Egress):    128
 IPV6 ACL Based QoS Policy Entries (Egress):    0
                            FCoE Egress ACL:    128
                          L2 MAC Classifier:    256
                     L2 MAC Classifier Prio:    0
                             VLN Classifier:    4096
                          Policy Classifier:    0
________________________________________________________

                current route table profile:    DEFAULT
________________________________________________________
                                ipv4_routes:    4096
                               max_nexthops:    1024
                                ipv6_routes:    1024
                        ipv4_neighbor_cache:    16384
                        ipv6_neighbor_cache:    4096
                         fcoe_domain_routes:    2048
________________________________________________________
```

VLAN considerations

- Before you configure an RSPAN session, you must create the RSPAN VLAN.
- A native VLAN cannot be made the RSPAN VLAN.
- The VLAN used for RSPAN should not be used for other purposes; furthermore, if the VLAN has ports as its members, it cannot be made an RSPAN VLAN. Only when the session is deconfigured, and the VLAN is deleted as an RSPAN VLAN, should the VLAN number be used for another purpose.
- You can configure any VLAN as an RSPAN VLAN as long as all participating network devices support the configuration of RSPAN VLANs and you use the same RSPAN VLAN for each RSPAN session in all participating network devices.
- You must configure the RSPAN VLANs on all source, intermediate, and destination network devices.
- Do not configure any ports in an RSPAN VLAN except the ports selected to carry RSPAN traffic. However, all configurations are allowed on the RSPAN destination port.
- The **vlan-id** of the packets marked for RSPAN will change to the RSPAN vlan-id.
- Access ports can be added to an RSPAN VLAN as destination ports.
- MAC address learning is disabled in the RSPAN VLAN.

Configuring SPAN

Refer also to Standard SPAN guidelines and limitations on page 33.

Configuring ingress SPAN

To configure SPAN for incoming packets only, do the following:

1. Open a monitor session and assign a session number.

   ```
   switch(config)# monitor session 1
   ```

2. Configure the source port and the destination port, with the **rx** parameter for received packets.

   The destination port is always an external port.

   ```
   switch(config-session-1)# source tengigabitethernet 1/0/15 destination tengigabitethernet 1/0/18
   direction rx
   ```

   NOTE
   If the following error is displayed, use the **lldp disable** command in interface subtype configuration mode to disable LLDP on the destination port before preceding: `% Error: Destination port cannot be in L2/L3/Qos/ACL/802.1x/LAG member/Lldp/Port-profile/non-default-MTU`.

3. Optional: Use the **description** command to add a label to the monitor session.

   ```
   switch(config-session-1)# description Hello World!
   ```

4. Optional: Repeat steps 1 and 2 as needed for additional ports.

   A monitor session can have only one source port. For additional ports you must create additional monitor sessions as needed for additional port mirroring sessions.

Configuring egress SPAN

To configure SPAN for outgoing packets only, do the following.

1. Open a monitor session and assign a session number

   ```
   switch(config)# monitor session 1
   ```

2. Configure the source port and the destination port, with the **tx** parameter for transmitted packets.

   The destination port is always an external port.

   ```
   switch(config-session-1)# source tengigabitethernet 1/0/15 destination tengigabitethernet 1/0/18
   direction tx
   ```

   NOTE
   If the following error is displayed, use the interface **lldp disable** command to disable LLDP on the destination port before preceding: `% Error: Destination port cannot be in L2/L3/Qos/ACL/802.1x/LAG member/Lldp/Port-profile/non-default-MTU`.

3. Optional: Use the **description** command to add a label to the monitor session.

   ```
   switch(config-session-1)# description Hello World!
   ```

4. Optional: Repeat steps 1 and 2 as needed for additional ports.

   A monitor session can have only one source port. For additional ports you must create additional monitor sessions as needed for additional port mirroring sessions.

Configuring bidirectional SPAN

To configure SPAN for packets traveling in both directions, do the following.

1. Open a monitor session and assign a session number

   ```
   switch(config)# monitor session 1
   ```

2. Configure the source port and the destination port, with the **both** parameter for all packets.

   The destination port is always an external port.

   ```
   switch(config-session-1)# source tengigabitethernet 1/0/15 destination tengigabitethernet 1/0/18
   direction both
   ```

   NOTE
   One of the following error messages may appear. If so, use the interface **lldp disable** command to disable LLDP on the destination port before preceding.

- % Error: Destination port cannot have LLDP configuration on it.
- % Error: Destination port cannot be in L2/L3/Qos/ACL/802.1x/LAG member/Lldp/Port-profile/non-default-MTU.

3. Optional: Use the **description** command to add a label to the monitor session.

   ```
   switch(config-session-1)# description Hello World!
   ```

4. Optional: Repeat steps 1 and 2 as needed for additional ports.

   A monitor session can have only one source port. For additional ports you must create additional monitor sessions as needed for additional port mirroring sessions.

Deleting a SPAN connection from a session

To remove a single connection from a SPAN session, do the following.

1. Display the existing configuration of the monitor session.

   ```
   switch# show monitor session 1
   ```

2. Open an existing monitor session.

   ```
   switch(config)# monitor session 1
   ```

3. Use the **no** keyword to delete a particular port connection.

   ```
   switch(config-session-1)# no source tengigabitethernet 1/0/15 destination tengigabitethernet 1/0/18
   direction both
   ```

4. Display the monitor session again to confirm the deletion of the connection.

   ```
   switch# show monitor session 1
   ```

Deleting a SPAN session

To remove a SPAN session, do the following:

1. Display the existing configuration of the monitor session.

   ```
   switch# show monitor session 1
   ```

2. Delete the existing monitor session by using the **no monitor session** command.

   ```
   switch(config)# no monitor session 1
   ```

3. Return to Privileged EXEC mode with the **exit** command.

4. Display the monitor session again to confirm the deletion of the connection.

   ```
   switch# show monitor session 1
   ```

Configuring RSPAN

Refer also to RSPAN guidelines and limitations on page 35.

The principal difference between configuring SPAN and RSPAN is that RSPAN requires a remote VLAN to be created first, by means of the **rspan-vlan** command. This example demonstrates the configuration of a bidirectional RSPAN.

1. Create a remote VLAN on the destination interface.

   ```
   switch(config)# interface vlan 100
   ```

2. Execute the **rspan-vlan** command to make the VLAN remote.

   ```
   switch(config-vlan-100)# rspan-vlan
   ```

3. Exit the VLAN configuration mode.

   ```
   switch(config-vlan-100)#end
   ```

4. Open a monitor session and assign a session number

   ```
   switch(config)# monitor session 1
   ```

5. Configure the source port and the destination port, with the **both** parameter for bidirectional port mirroring.

   By modifying the direction parameter, you can control whether this is an ingress, egress, or a bidirectional SPAN.

   In the case of RSPAN, the destination is the VLAN, instead of a destination interface.

   ```
   switch(config-session-1)# source tengigabitethernet 1/0/15 destination rspan-vlan 100 direction both
   ```

6. Optional: Use the **description** command to add a label to the monitor session.

   ```
   switch(config-session-1)# description Hello World!
   ```

7. Use the **switchport** command to add a port to the RSPANVLAN to access the mirrored packets.

   ```
   switch(config-session-1)# exit
   switch (config)# interface ten 1/0/15
   switch(conf-if-te-1/0/15)# switchport access rspan-vlan 100
   ```

8. Display the results of the configuration.

   ```
   switch(conf-if-te-1/0/15)# do show vlan rspan-vlan
   ```

Flow-based SPAN and RSPAN

You can snoop on traffic that passes through a particular port, using flow-based SPAN or RSPAN to copy the packets to a port connected to the analyzer.

Flow-based SPAN selectively mirrors the traffic coming on the source port that matches an ACL-based filter to a destination port, which can be a local node or remote node to support RSPAN.

For example, assume there are two streams of traffic, one from the source Mac1 and other from source Mac2 are being forwarded from port te1/0/1 to port te1/0/2 . You can, with the help of an ACL to permit only source Mac1 traffic, configure a flow-based SPAN session with the source on port te1/0/1 and port te1/0/2 as the destination port. All traffic coming in on port te1/0/1 originating from source Mac1 will be duplicated and sent to port te1/0/2. No mirroring occurs for traffic originating from source Mac2.

Consider the following guidelines and restrictions for flow-based SPAN and RSPAN:

- Flow-based SPAN source port cannot be an ISL port.
- Bi-directional association of the service policy cannot be supported with the current infrastructure. You must apply the service policy in both directions in two separate commands.
- Port-based or VXLAN-based SPAN sessions cannot be specified as the SPAN action.
- Deny rules in an service ACL is a pass through in flow-based QoS. Only permit rules with SPAN action result in flow-based SPAN.
- If a rule is configured as permit in flow-based ACL with SPAN action and the same rule is configured as deny in a user policy, the packet is dropped as per the user policy and the same is mirrored to the SPAN destination port.
- In a class map, if the SPAN action co-exists with any other QoS action (such as DSCP marking which results in frame editing), the mirrored packet is the original packet and hence does not reflect the frame editing done, as per the QoS action.

Configuring flow-based SPAN and RSPAN

You can replicate traffic from a defined source and direct it to snooping software on a designated port.

This task assumes you have already completed the following tasks:

- You have already created a policy map instance.
- You have already created a class map for the policy map.

To configure flow-based SPAN, perform the following task in privileged EXEC mode.

1. Enter global configuration mode.

   ```
   switch# configure terminal
   ```

2. Create the monitor session.

   ```
   switch(config)# monitor session 1
   ```

3. Set the destination port for the replicated traffic for SPAN.

   NOTE
   Remote ports are supported for RSPAN. Use the **rspan** *vlan_id* variable to configure for RSPAN.

   ```
   switch(config)# destination rspan 100
   ```

4. Activate the pre-defined policy map.

   ```
   switch(config)# policy-map policymap
   ```

5. Activate the pre-defined class for the policy map.

   ```
   switch(config-policymap)# class policyclass
   ```

6. Activate the span session and assign it an identifying number.

```
switch(config-policyclass)# span session 1
```

7. Return to global configuration mode by executing the **exit** command twice.

```
switch(config-policyclass)# exit
switch(config-policymap)# exit
switch(config)#
```

8. Enter configuration mode for the source interface.

```
switch(config)#interface ten 1/0/1
```

9. Bind the policy to the interface.

```
switch(conf-te-1/0/1)# service-policy in policyclass
```

10. Confirm the session with the **show monitor** command.

```
switch# show monitor
Session                 : 1
Type                    : Remote source session
Description             : [None]
Session Type: Flow based
Enabled on Source Interfaces:
************************************
Ifname                                State      Direction
*************************************
gi1/0/2                                (Up)      Rx
te1/0/1                                (Up)      Rx
Destination Interface   : Vlan 100
```

Deleting the flow-based SPAN session

You remove the flow-based SPAN session by disassociating the span session from the policy-map . The pre-defined policy map and class as such are not deleted.

1. Activate the pre-defined policy map.

```
switch(config)# policy-map policymap
```

2. Unbind the session from the policy map.

```
switch(config)# no monitor session 1
```

3. Activate the pre-defined class for the policy map.

```
switch(config-policymap)# class policyclass
```

4. Deactivate the span session with the **no span session** version of the command and the identifying number.

```
switch(config-policyclass)# no span session 1
```

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.

```
switch# configure terminal
```

2. Configure the RMON event.

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

3. Return to privileged EXEC mode.

```
switch(config)# end
```

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

```
switch# 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.

> **NOTE**
> RMON configuration is not supported on breakout ports in Network OS versions prior to v6.0.0.

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.

   ```
   switch# configure terminal
   ```

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

   ```
   switch(config)# interface tengigabitethernet 1/0/1
   ```

3. Enable the DCB interface.

   ```
   switch(conf-if-te-1/0/1)# no shutdown
   ```

4. Configure RMON Ethernet group statistics on the interface.

   ```
   switch(conf-if-te-1/0/1)# rmon collection stats 200 owner john_smith
   ```

5. Return to privileged EXEC mode.

   ```
   switch(conf-if-te-1/0/1)# end
   ```

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

   ```
   switch# 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.

   ```
   switch# configure terminal
   ```

2. Configure the RMON alarms.

   Example of an alarm that tests every sample for a rising threshold

   ```
   switch(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

   ```
   switch(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.

   ```
   switch(config)# end
   ```

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

   ```
   switch# 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 tengigabitethernet 170/0/1
   device(conf-if-te-170/0/1)# rmon collection stats 2 owner admin
   ```

4. Use an appropriate RMON MIB for additional monitoring.

sFlow

Overview

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

The sFlow standard consists of an sFlow agent that resides anywhere within the path of the packet and an sFlow collector that resides on a central server. This release is compliant with sFlow Version 5.

The sFlow agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector at regular intervals. The datagrams consist of information on, but not limited to, packet header, ingress interfaces, sampling parameters, and interface counters. Packet sampling is typically performed by the ASIC. The sFlow collector analyzes the sFlow datagrams received from different devices and produces a network-wide view of traffic flows. You can configure up to five collectors, using both IPv4 and IPv6 addresses.

The sFlow datagram provides information about the sFlow version, its originating agent's IP address, a sequence number, one or more flow samples or counter samples or both, and protocol information.

The sFlow agent uses two forms of operation:

- Time-based sampling of interface counters
- Statistical sampling of switched packets

sFlow can be port based or 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.

Flow based sFlow ensures that sampling is done per flow instead of per port. Flow based sFlow uses sFlow profile sampling rate.

The following applications does flow based sFLow.

- User flow based sflow
- VxLAN visibility sflow

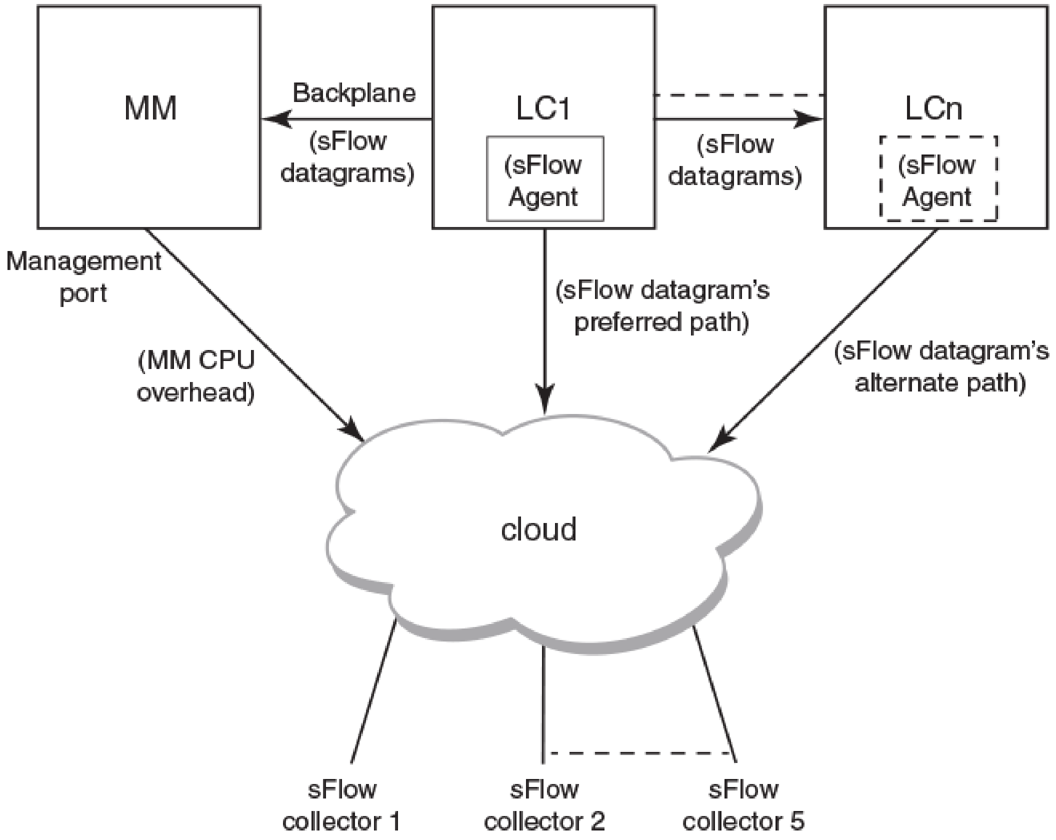
When flow based sFlow is enabled along with port based sFlow, port based sFlow will have higher precedence and only port based sFlow will work at this stage.

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).

sFlow datagram path to sFlow collectors



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 5 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).
Flow based sFLow	Supported Port-based and flow-based sFlow are supported on physical ethernet ports only.
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 scanning for inbound, outbound, or both directions on a port	Inbound only
Multiple collector configuration	A maximum of five IPv4 or IPv6 collectors could be configured and can be part of any of the configured VRFs.
Subagent-ID	Slot number of the interface
Agent IP address	Cannot be configured through CLI. Management CP IP is always used as the Agent IP address.
sFlow counter polling support on per-port, per-VLAN, or per-trunk or per tunnel basis	Supports per-port counter polling only.
All standard if_counters and Ethernet counters	Supported
AS path cleanup timer (v4: BGP communities, v5: BGP next hop router)	Not supported
sFlow support on VxLAN tunnels	Supported

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 flow 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
```

9. (Optional) Issue the **show running-config sflow** command to view the configuration.

   Following is a sample **show running-config sflow** command output.

```
devoce# show running-config sflow
sflow enable
sflow collector 10.10.10.100 6343 use-vrf default-vrf
sflow collector 10.252.200.219 6343 use-vrf mgmt-vrf
sflow collector 172.22.224.199 6343 use-vrf mgmt-vrf
sw0# show running-config sflow-profile
sflow-profile profile1 sampling-rate 2
device#
```

Enabling flow-based sFlow

Perform the following steps, beginning in global configuration mode.

NOTE
The "deny ACL" rule is not supported for flow-based sflow. Only the permit action is supported.

1. Create an sFlow profile. Be sure to specify the sampling-rate as a power of 2.

```
device(config)# sflow-profile profile1 sampling-rate 256
```

2. Create a standard MAC ACL.

```
device# mac access-list standard acl1
device(conf-macl-std)# permit any
```

3. Create a class map and attach the ACL to the class map.

```
device(conf-macl-std)# class-map class1
device(config-classmap)# match access-group acl1
```

4. Create a policy map and attach the class map to the policy map.

   ```
   device(config-classmap)# policy-map policy1
   device(config-policymap)# class class1
   ```

5. Use the **map** command to add an sFlow profile name.

   This example assigns the profile name "profile1."

   ```
   device(config-policymap-class)# map sflow profile1
   ```

6. Switch to interface configuration mode.

   ```
   device(config-policymap-class)# exit
   device(config)# interface ten 1/8/1
   device(conf-if-te-1/8/1)#
   ```

7. Bind the policy map to an interface.

   ```
   device(conf-if-te-1/8/1)# service-policy in policy1
   ```

8. (Optional) Issue the **show running-config sflow-profile** command to view the configured sFlow profile.

   ```
   device# show running-config sflow-profile
   sflow-profile profile1 sampling-rate 256
   device#
   ```

Disabling flow-based sFlow on specific interfaces

To disable sFlow on a specific interface, perform the following steps in interface configuration mode.

1. Switch to interface configuration mode.

   ```
   device(config)# interface ten 1/8/1
   device(conf-if-te-1/8/1)#
   ```

2. Disable flow-based sFlow by removing the policy map.

   ```
   device(conf-if-te-1/8/1)# no service-policy in
   ```

3. Confirm the sFlow configuration status on the specific interface.

   ```
   device# show sflow interface tengigabitethernet 1/8/1
   ```

Configuring sFlow for interfaces

After the global sFlow configuration, sFlow must be explicitly enabled on all the required interface ports.

> NOTE
> When sFlow is enabled on an interface port, it inherits the sampling rate and polling interval from the global sFlow configuration.

Enabling and customizing sFlow on specific interfaces

Perform the following steps in privileged EXEC mode to enable and customize sFlow on an interface. This task assumes that sFlow has already been enabled at the global level.

1. Enter the **interface** command to specify the DCB interface type, the RBridge ID, and the slot/port number.

   ```
   device(config)# interface tengigabitethernet 1/0/24
   ```

2. Use the **sflow enable** command to enable sFlow on the interface.

   ```
   device(conf-if-te-1/0/24)# sflow enable
   ```

3. Configure the sFlow polling interval.

   ```
   device(conf-if-te-1/0/24)# sflow polling interval 35
   ```

4. Set the sFlow sample-rate.

   ```
   device(conf-if-te-1/0/24)# sflow sample-rate 8192
   ```

5. (Optional) Confirm the sFlow configuration status on the specified interface using the **show sFlow interface** command.

   Following is a sample output of the **show sFlow interface** command.

   ```
   device# show sflow interface tengigabitethernet 1/0/24

   sFlow info for interface TenGigabitEthernet 1/0/24
   ------------------------------------------------
   Port based sflow services are:         enabled
   Flow based sflow services are:         disabled
   Configured sampling rate:              8192 pkts
   Actual sampling rate:                  8192 pkts
   Counter polling interval:              35 secs
   Samples received from hardware:        0
   Port backoffThreshold :                1024
   Counter samples collected :            1

   device#
   ```

Configuring an sFlow policy map and binding it to an interface

Perform the following steps to configure an sFlow policy map and bind it to an interface.

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

   ```
   switch# configure terminal
   ```

2. Create a standard MAC access control list (ACL).

   ```
   switch# mac access-list standard acl1
   switch(conf-macl-std)# permit any
   ```

3. Create a class map and attach the ACL to the class map.

   ```
   switch(conf-macl-std)# class-map class1
   switch(config-classmap)# match access-group acl1
   ```

4. Create a policy map and attach the class map to the policy map.

   ```
   switch(config-classmap)# policy-map policy1
   switch(config-policymap)# class class1
   ```

5. Add an sFlow profile name by using the **map** command.

   This example assigns the profile name "policy1."

   ```
   switch(config-policymap-class)# map sflow policy1
   ```

6. Bind the policy map to an interface.

   ```
   switch(conf-if-te-1/8/1)# service-policy in policy1
   ```

Disabling sFlow on specific interfaces

To disable sFlow on a specific interface, perform the following steps in interface configuration mode.

1. Disable the sFlow interface.

   ```
   switch(conf-if)# no sflow enable
   ```

2. Return to privileged EXEC mode.

   ```
   switch(conf-if)# end
   ```

3. Confirm the sFlow configuration status on the specific interface.

   ```
   switch# show sflow interface tengigabitethernet 5/0/12
   ```

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:                      enabled
Global default sampling rate:            32768 pkts
Global default counter polling interval: 20 secs
Rbridge-Id                           Collector server address         Vrf-Name       Samples sent
--------------------------------------------------------------------------------------------------
         2                                   10.1.15.2:6343           default-vrf        0
         2                                   100.1.1.2:6343           red-vrf               0
         2                               172.22.108.57:6343           mgmt-vrf           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(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
```

Syslog

Syslog overview

Syslog messages are triggered by events and contain information at various levels of event severity.

Software installed ina device can write syslog messages to provide information at the following severity levels:

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

The device writes the messages to a local buffer, which can hold up to 5000 entries.

To view the actual Syslog messages, refer to the *Extreme Network OS Message Reference*.

System Monitoring

System Monitor overview

System Monitor provides customizable monitoring thresholds, which allow you to monitor the health of each component of a switch. Whenever a switch 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. In Network OS 4.0.0 and later, it is possible to monitor individual switches in a logical chassis cluster or fabric cluster. This is done in RBridge ID configuration mode, by addressing the RBridge ID of the selected switch.

Threshold and notification configuration procedures are described in the following sections.

Monitored components

The following FRUs and temperature sensors are monitored on supported switches:

- **LineCard** —Displays the threshold for the line card.
- **MM** —Displays the threshold for the management module.
- **SFM** —Displays the threshold for the switch fabric module device.
- **cid-card** —Displays the threshold for the chassis ID card component.
- **compact-flash** —Displays the threshold for the compact flash device.
- **fan** —Configures fan settings.
- **power** —Configures power supply settings.
- **sfp** —Displays the threshold for the small form-factor pluggable (SFP) device.
- **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 switch 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.

> NOTE
> For details about each RASLog message, refer to the "RAS System Messages" chapter of the *Network OS Message Reference*.

The following table lists the marginal and down thresholds for components monitored by System Monitor on supported switches.

TABLE 6 Hardware platform marginal and threshold settings for supported switches

Platform	Hardware component	Marginal threshold	Down threshold
Extreme VDX 6740	Power supply	1	2
	Temperature sensor	1	2
	Compact flash	1	0
	Fan	1	2
Extreme VDX 8770-4	Power supply	1	2
	Temperature sensor	1	2
	Compact flash	1	0
	Fan	1	2
Extreme VDX 8770-8	Power supply	6	7
	Temperature sensor	1	2
	Compact flash	1	0
	Fan	1	2

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 *Network 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 63.)

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter RBridge ID configuration mode, as in the following example.

   ```
   switch(config)# rbridge-id 154
   ```

3. Change **down-threshold** and **marginal-threshold** values for the SFM.

   ```
   switch(config-rbridge-id-154)# 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. Enter RBridge ID configuration mode (for RBridge ID 154 in this case).

   ```
   switch(config)# rbridge-id 154
   ```

To enable a RASLog alert when the power supply is removed, enter the following command:

```
switch(config-rbridge-id-154)# 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, SFP, interface, and security 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 switches in a logical chassis cluster. For complete information on the **system-monitor-mail relay host** command, refer to the *Network 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.

```
switch(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 switch to resolve the domain name and forward all e-mail messages to a relay server.

- To create a mapping:

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

- To delete the mapping:

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

- To change the domain name:

  ```
  switch(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:

  ```
  switch(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 switch health status

To display the health status of a switch, enter **show system monitor**.

```
switch# show system monitor
** System Monitor Switch Health Report **
RBridge 154     switch status            : MARGINAL
                Time of Report           : 2013-03-24 20:51:53
                Power supplies monitor   : MARGINAL
                Temperatures monitor     : HEALTHY
                Fans monitor             : HEALTHY
                Flash monitor            : HEALTHY
```