Extreme

Customer-Driven Networking

Extreme SLX-OS Monitoring Configuration Guide, 17s.1.02

Supporting the ExtremeSwitching SLX 9140 and SLX 9240 Switches

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.

Extreme SLX-OS Monitoring Configuration Guide, 17s.1.02
53-1005314-02

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

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 this SLX-OS release, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- ExtremeSwitching SLX 9140
- ExtremeSwitching SLX 9240

   NOTE
   Some of the commands in this document use a slot/port designation. Because the SLX 9140 and the SLX 9240 do not contain line cards, the slot designation must always be "0" (for example, 0/1 for port 1).

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.

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.

SPAN guidelines and limitations

Consider the following topics when configuring SPAN.

Standard SPAN guidelines and limitations

TABLE 1 Number of SPAN sessions supported under various conditions

Extreme platform	Number of RX or TX span sessions without shared destination	Number of both direction span sessions without shared destination	Number of span sessions with same direction and shared destination
SLX-9140/9240	4	2	8

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

- The mirror port should not be configured to carry normal traffic.
- The destination mirror port can handle up to 100 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 Inter-Chassis Link (ICL) is supported.
- Mirroring of LAG or port-channel interfaces is not supported, but LAG members can be mirrored.
- Ethernet Pause frames are not mirrored.
- 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 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, , 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.

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

Configuring SPAN

Refer also to Standard SPAN guidelines and limitations on page 11.

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 ethernet 0/1 destination ethernet 0/2 direction rx
```

   NOTE
   If the following error is displayed, use the **lldp disable** or related configuration command in interface subtype configuration mode to disable LLDP or other related configuration on the destination port before preceding: `%`
   `Error: Destination port cannot have L2/L3/Qos/ACL/802.1x/LAG/LLDP/Port-profile/MTU/`
   `StormControl/RMON configuration on it..`

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 ethernet 0/1 destination ethernet 0/2 direction tx
   ```

   > **NOTE**
   > If the following error is displayed, use the interface **lldp disable** or related configuration command to disable LLDP or other related configuration on the destination port before preceding: `% Error: Destination port cannot have L2/L3/Qos/ACL/802.1x/LAG/LLDP/Port-profile/MTU/StormControl/RMON configuration on it..`

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 ethernet 0/1 destination ethernet 0/2 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 have L2/L3/Qos/ACL/802.1x/LAG/LLDP/Port-profile/MTU/StormControl/RMON configuration on it.

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 ethernet 0/1 destination ethernet 0/2 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
   ```

Flow-based SPAN

You can snoop on traffic that passes through a particular port, using flow-based SPAN 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.

For example, assume there are two streams of traffic, one from the source Mac1 and other from source Mac2 are being forwarded from eth 0/1 eth 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:

- Only ingress direction of the service policy is supported with the current infrastructure.
- Port-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

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.

   ```
   device# configure terminal
   ```

2. Create the monitor session.

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

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

   ```
   device(config-session-1)# destination ethernet 0/2
   ```

4. Activate the pre-defined policy map.

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

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

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

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

   ```
   device(config-policymap-class)# span session 1
   ```

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

   ```
   device(config-policymap-class)# exit
   ```

8. Enter configuration mode for the source interface.

   ```
   device(config)#interface ethernet 0/1
   ```

9. Bind the policy to the interface.

   ```
   device(conf-if-eth-0/1)# service-policy in policymap
   ```

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

```
device# show monitor

Session               : 1
Description           : [None]
Type                  : Flow Based SPAN
Enabled on the source interfaces
***************************************************
Name                  State      Direction
***************************************************
Eth 0/1               (Up)       Rx
Destination Interface  : Eth 0/2 (Up)
device#
```

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.

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

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

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

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

```
device(config-policymap-class)# no span session 1
```

4. Delete the span session.

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

Network Elements Telemetry

Network elements telemetry overview

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

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

Streaming of telemetry data

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

Streaming telemetry is supported using the following two approaches:

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

Encoding formats

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

Telemetry profiles

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

System profile

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

Interface profile

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

Supported telemetry data

The following system-related telemetry data classifications are supported.

System data

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

Interface counters

Interface counters are supported on physical interfaces only.

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

Streaming telemetry data using a gRPC server

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

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

Streaming telemetry data to a collector profile

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

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

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

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

The collector profile defines collector-related information as:

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

Telemetry Secure Certificate Management

Telemetry supports secure monitoring through SSL transport security.

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

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

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

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

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

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

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

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

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

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

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

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

-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoMB0Jyb2NhZGUxEjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xNzAzMjExNzQ1NDNa
Fw0xODAzMjExNzQ1NDNaMDMxCzAJBgNVBAYTAkNBMRAwDgYDVQQKDAdCcm9jYWRl
MRIwEAYDVQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC+YG/CkiNm/BO+u1mYLKP8cpz/OO9CE+fusO0spXxjKfjPAvK7kiogxABm
bg9MQeWl4SbFa5x3q5uyZJxApJ+tAnnWZa+cbj5pmNsQFfIbFOwSAmFyhh/NIp7Y
/wApskKjnVsMFkarqX8W2xKxZreapZFMa9DGpOeh8Jo2yvcTAimFfSJ4nyKlCr1C
DuuaTSvAttC8Z9mEqD9TOaSYwQI0pnfVO+ySgY8ndqDXYdRvl+bV1taghlKOgxMY
J78lyZxYf6CIn22BAaz/f9a5ffS13Hh5Cmurj2dUmmqDE49p2KEVtXQ3D6nuopli
V49ok+z93/40Uq4OVJZJk5Kx8ZuxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAI1d
1VkMH9i3SorPIHpbVqbeDe7LPdaFmrT0COr3AFUECw3gBj1Zy82Kp8XkIJJdVCu8
MNm3wTARqeNBY2c3luw6QeA6l4qRIVM4FqNj6rvtqtNZQ9EEKRRwAm0GSVp+uSvu
E88XSXO+r6N+SXQemRIyhNQ7LJq+cDEaP5WfNtKg+zj085Xd0qiB94BKFt5Q+xAa
B7lwuUvT7Yt92aUVXIaZ6aY5oMv4t7+lPBBKjg8cNeywDa9h3yVZYIzSggghu0qu
GZO57qUh5agxqKiEVf9Ya325u5gj73UJsKOSsyVA1HB8RsPEEdz8j8FBAqMNSTQj
8UDtUGpYiYlzyiBUELc=
-----END CERTIFICATE-----
```

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

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

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

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

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

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

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

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

-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoMB0Jyb2NhZGUxEjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xNzAzMjExNzQ1NDNa
Fw0xODAzMjExNzQ1NDNaMDMxCzAJBgNVBAYTAkNBMRAwDgYDVQQKDAdCcm9jYWRl
MRIwEAYDVQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC+YG/CkiNm/BO+u1mYLKP8cpz/0O9CE+fusO0spXxjKfjPAvK7kiogxABm
bg9MQeWl4SbFa5x3q5uyZJxApJ+tAnnWZa+cbj5pmNsQFfIbFOwSAmFyhh/NIp7Y
/wApskKjnVsMFkarqX8W2xKxZreapZFMa9DGpOeh8Jo2yvcTAimFfSJ4nyKlCr1C
DuuaTSvAttC8Z9mEqD9TOaSYwQI0pnfVO+ySgY8ndqDXYdRvl+bV1taghlKOgxMY
J78lyZxYf6CIn22BAaz/f9a5ffS13Hh5Cmurj2dUmmqDE49p2KEVtXQ3D6nuopli
V49ok+z93/40Uq4OVJZJk5Kx8ZuxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAI1d
1VkMH9i3SorPIHpbVqbeDe7LPdaFmrT0COr3AFUECw3gBj1Zy82Kp8XkIJJdVCu8
MNm3wTARqeNBY2c3luw6QeA6l4qRIVM4FqNj6rvtqtNZQ9EEKRRwAm0GSVp+uSvu
E88XSXO+r6N+SXQemRIyhNQ7LJq+cDEaP5WfNtKg+zj085Xd0qiB94BKFt5Q+xAa
B7lwuUvT7Yt92aUVXIaZ6aY5oMv4t7+lPBBKjg8cNeywDa9h3yVZYIzSgghu0qu
GZO57qUh5agxqKiEVf9Ya325u5gj73UJsKOSsyVA1HB8RsPEEdz8j8FBAqMNSTQj
8UDtUGpYiYlzyiBUELc=
-----END CERTIFICATE-----
device(config-server-mgmt-vrf)# transport ssl
device(config-server-mgmt-vrf)# do show telemetry server status

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

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

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

Configuring telemetry profiles

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

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

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

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

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

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

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

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

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

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

   For information on all the attributes of the **interface** refer to the *Command Reference*.

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

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

   For information on all the attributes of the **interval** refer to the *Command Reference*

   .

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

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

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

The following is a complete telemetry profile configuration example.

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

Configuring the telemetry collectors

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

Configure the telemetry profiles before configuring the telemetry collector.

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

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

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

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

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

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

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

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

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

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

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

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

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

   Telemetry data is streamed to collector_1 on 10.128.116.10 and port 1, with transport as tcp.

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

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

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

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

The following is a complete telemetry collection configuration example.

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

Telemetry data is streamed to collector_1 on 10.128.116.10 and port 1, with transport as tcp.

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

Configuring telemetry servers

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

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

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

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

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

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

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

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

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

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

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

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

The following is a complete telemetry server configuration example.

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

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

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

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

Hardware Monitoring

Hardware monitoring overview

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

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

System Resource Monitoring (SRM)

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

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

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

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

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

```
device(config)# resource-monitor cpu
Possible completions:
  action      Action to take when CPU usage exceeds threshold
  enable      Enable monitoring CPU usage
  threshold   Threshold for high CPU usage
device(config)# resource-monitor cpu enable
Possible completions:
  action      Action to take when CPU usage exceeds threshold
  threshold   Threshold for high CPU usage
  <cr>
device(config)# resource-monitor cpu enable action raslog threshold
Possible completions:
  <PERCENT:70-100 percent CPU being busy>[90]
device(config)# resource-monitor cpu enable action raslog threshold
```

For more information on commands, please refer the *SLX-OS Command Reference* guide for the SLX 9140 and 9240 Switches.

Configuring system resource monitoring

Execute the following steps to configure resource monitoring.

1. Enter global configuration mode.

    ```
    device# configure terminal
    ```

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

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

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

    ```
    device(config)# resource-monitor memory enable action raslog threshold 80
    ```

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

    ```
    device(config)# resource-monitor process memory  enable alarm 800 critical 1000
    ```

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

    ```
    device# show running-config resource-monitor
     resource-monitor cpu enable
     resource-monitor memory enable threshold 80 action raslog
     resource-monitor process memory enable alarm 800 critical 1000
    !
    device#
    ```

CPU, memory, and buffer monitoring

SRM allow users to enable or disable the CPU and memory monitoring services and set threshold values. By default, these services are enabled.

With CPU monitoring service enabled, if the system CPU is busy and reaches certain threshold, a RASLOG message is generated. This is informational only and no user action is required.

With the system memory monitoring service enabled, if the system memory is running low and goes below the threshold in the system, SRM notifies the user via RASLOG message. This RASLOG message allows the user to investigate any potential system memory issues easily.

With the process memory monitoring service enabled, if any of the process consumes too much memory and the usage reaches certain threshold, a WARNING message is generated. If the usage still goes up to another threshold, a CRITICAL message will be generated. These RASLOG messages allow the user to identify any potential process resource issues.

Configuring hardware monitoring for CPU, memory, and buffer usage

Alerts can be set for cpu, memory, and buffer usage.

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

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

1. Enter global configuration mode.

```
device# configure terminal
```

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

3. 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.

Viewing threshold status

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

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

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

```
device# show defaults threshold interface type Ethernet

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

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 0/1      connected (up)  --      10G     10G-SFP-SR
Eth 0/2      adminDown     --        --      --
Eth 0/3      notconnected  --        --      10G-SFP-SR
Eth 0/4      port-crcDown  --        --      --
```

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

```
device# show interface ethernet 0/4
Ethernet 0/4 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 0/1        10.3.1.1      default-vrf         up                     up
Ethernet 0/2        unassigned    default-vrf         port-crc down          down
Ethernet 0/3        10.3.3.1      default-vrf         up                     down
Ethernet 0/4        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 0/4
 Ethernet 0/4 is port-crc down protocol is down
 IP unassigned
 Proxy Arp is not Enabled
 Vrf : default-vrf
```

For more information on commands, refer the *SLX-OS Command Reference* for the SLX 9140 and 9240 Switches.

Beacon LED support

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

Beacon LED can be configured in following two ways:

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

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

Remote Monitoring

RMON overview

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

Configuring and managing RMON

Both alarms and events are configurable RMON parameters.

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

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

Configuring RMON events

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

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

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

   ```
   device# configure terminal
   ```

2. Configure SNMP v2c.

   ```
   device(config)# snmp-server enable trap
   device(config)# snmp-server view all 1 included
   device(config)# snmp-server community public groupname group2
   device(config)# snmp-server group group2 v2c read all write all notify all
   sw0(config)# snmp-server user user2 groupname group2
   sw0(config)# snmp-server host <host-name> public version 2c severity-level Info
   sw0(config-host-<host-name>/public)# exit
   ```

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

   ```
   device(config)# rmon event 100 description hi_100 log trap public owner john_smith
   device(config)# rmon event 101 description lo_100 log trap public owner john_smith
   ```

4. Return to privileged EXEC mode.

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

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

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

Configuring RMON Ethernet group statistics collection

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

Ethernet group statistics collection is not supported on ISL links.

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

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

```
device# configure terminal
```

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

```
device(config)# interface ethernet 0/32:1
device(conf-if-eth-0/32:1)# no shutdown
```

3. Configure RMON collection history using the **rmon collection history** command.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-te-0/1)# rmon collection history 5 interval 120 owner admin
```

4. Configure RMON Ethernet group statistics on the interface.

```
device(conf-if-eth-0/32:1)# switchport
device(conf-if-eth-0/32:1)# rmon collection stats 100 owner john_smith
```

5. Return to privileged EXEC mode.

```
device(conf-if-eth-0/32:1)# end
```

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

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

Configuring RMON alarm settings

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

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

```
device# configure terminal
```

2. Configure the RMON alarms.

   Following is an example of an alarm that tests every sample for rising threshold and falling threshold.

   ```
   device(config)# rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.100 interval 10 absolute rising-threshold
   10000 event 100 falling-threshold 5000 event 101 owner john_smith
   ```

   Delta alarms can be configured as follows.

   ```
   device(config)# rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.100 interval 5 delta rising-threshold 2000
   event 100 falling-threshold 1000 event 101 owner john_smith
   device(config)# rmon alarm 200 1.3.6.1.2.1.16.1.1.1.5.200 interval 5 delta rising-threshold 2000
   event 200 falling-threshold 1000 event 201 owner john_smith
   ```

   The events are not triggered when alarms are configured with invalid OIDS.

3. Return to privileged EXEC mode.

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

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

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

5. To view configured alarms, use the **show running-config rmon alarm** command.

Monitoring CRC errors

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

The following synchronizes the statistics maintained for the interface and RMON, as well as ensures proper reporting from an operational standpoint.

1. Issue the **clear counters all** command in global configuration mode.

   ```
   device# clear counters all
   ```

2. Issue the **clear counters rmon** command.

   ```
   device# clear counters rmon
   ```

3. Execute the **rmon collection stats** command on each interface, as in the following example.

   ```
   device(config)# interface ethernet 0/1
   device(conf-if-eth-0/1)# rmon collection stats 2 owner admin
   ```

   > **NOTE**
   > The CRC OID is 1.3.6.1.2.1.16.1.1.1.8. While configuring the alarm, this OID may be used for both delta and absolute alarms.

4. Use an appropriate RMON MIB for additional monitoring.
   For example, to obtain CRC statistics on a Extreme SLX-OS platform, the following RMON MIB could be used: Object-etherStatsCRCAlignErrors, OID- .1.3.6.1.2.1.16.1.1.1.8

Viewing RMON logs, events, alarms, and statistics

Following show commands enable you to view the RMON logs, events, alarms, and statistics.

- **show rmon logs**

```
device(config)# do show rmon logs
event Index = 100
        log Index = 1
        log generated time = 00:05:50 (35000)
        log description rising_100

event Index = 101
        log Index = 1
        log generated time = 00:05:30 (33000)
        log description falling_100
```

- **show rmon events**

```
device(config)# do show rmon events
event Index = 100
Description rising_100
        Event type Log
        Last Time Sent = 00:05:50
        Owner  john_smith

event Index = 101
Description falling_100
        Event type Log
        Last Time Sent = 00:05:30
        Owner  john_smith
```

- **show rmon alarms**

```
device(config)# do show rmon alarms
alarm Index = 100
        alarm status = VALID
        alarm Variable = 1.3.6.1.2.1.16.1.1.1.5.100
        alarm Interval = 10
        alarm Type is Absolute
        alarm Value  = 10000
        alarm Rising Threshold = 10000
        alarm Rising Event = 100
        alarm Falling Threshold = 5000
        alarm Falling Event = 101
        alarm Owner is john_smith
```

- **show rmon statistics**

```
device(config)# do show rmon statistics
rmon collection index 100
    Interface index is Id: 201589376 , Name : Ethernet 0/32:1
    Receive Statistics:
        10000 packets, 1280000 bytes,  0 packs dropped
        Multicasts: 0, Broadcasts: 0

        Under-size : 0, Jabbers: 0, CRC: 0
        Fragments: 0, Collisions: 0

        64 byte pkts: 0, 65-127 byte pkts: 0
        128-255 byte pkts: 10000, 256-511 byte pkts: 0
        512-1023 byte pkts: 0, 1024-1518 byte pkts: 0
        Over 1518-byte pkts(Oversize - Jumbo): 0

    Owner: RMON_SNMP
    Status: ok(1)
```

System Monitoring

System Monitor overview

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

Because of platform-specific values that vary from platform to platform, it was previously not possible to configure platform-specific thresholds through a global CLI command.

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

Monitored components

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

- **cid-card**—Displays the threshold for the chassis ID card component.
- **compact-flash**—Displays the threshold for the compact flash device.
- **fan**—Configures fan settings.
- **power**—Configures power supply settings.
- **temp**—Displays the threshold for the temperature sensor component.

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

Monitored FRUs

System Monitor monitors the absolute state of the following FRUs:

- Fan
- Power supply
- CID card

Possible states for all monitored FRUs are removed, inserted, on, off, and faulty. A state of none indicates the device is not configured. If the FRU is removed, inserted, or goes into a faulty state, System Monitor sends a RASLog message or an e-mail alert, depending on the configuration. The health status of the FRU being monitored is not affected by the on or off status. The System Monitor generates a separate RASLog message for the overall health of the device. Use the **show system monitor** command to view the health status of a device. Refer to the *Displaying the device health status* section for example output.

SFM monitoring

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

Configuring System Monitor

This section contains example basic configurations that illustrate various functions of the **system-monitor** command and related commands.

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 38.)

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

   > **NOTE**
   > You can disable the monitoring of each component by setting **down-threshold** and **marginal-threshold** values to 0 (zero).

Setting state alerts and actions

System Monitor generates an alert when there is a change in the state from the default or defined threshold.

1. Issue the **configure terminal** command to enter global configuration mode.
2. To enable a RASLog alert (example: when the power supply is removed), enter the following command:

   > **NOTE**
   > There are no alerts for MM, compact-flash, or temp. There are no alert actions for SFPs.

Configuring e-mail alerts

Use the **system-monitor-mail fru** command to configure e-mail threshold alerts for FRU and optic monitoring. For an e-mail alert to function correctly, you must add the IP addresses and host names to the domain name server (DNS) in addition to configuring the domain name and name servers. For complete information on the **system-monitor-mail relay host** command, refer to the *Extreme SLX-OS Command Reference* for the SLX 9140 and 9240 Switches

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter the following command to enable e-mail alerts and to configure the e-mail address.

```
device(config)# system-monitor-mail fru enable email-id
```

Sendmail agent configuration

The sendmail agent must have one of the following configuration to resolve the domain-name.

- Configure DNS settings to connect device to DNS server.

- In case if DNS server is not available, DNS configuration along with relay host configuration is required for the sendmail agent on the device to resolve the domain-name. E-mail can be forwarded through the relay host. For example:

```
device(config)# ip dns domain-name corp.Extreme.com
device(config)# ip dns name-server 10.70.20.23
device(config)# ip dns name-server 10.70.20.43
```

The following **system-monitor-mail relay host** commands allow the sendmail agent on the device to resolve the domain name and forward all e-mail messages to a relay server.

- To create a mapping:

```
device(config)# system-monitor-mail relay 10.70.212.167 domain-name scooby.Extreme.com
```

- To delete the mapping:

```
device(config)# no system-monitor-mail relay 10.70.212.167 domain-name scooby.Extreme.com
```

- To change the domain name:

```
device(config)# system-monitor-mail relay 10.70.212.167 domain-name domain_name2.Extreme.com
```

> **NOTE**
> You must delete the first domain name before you can change it to a new domain name.

- To delete the domain name and return to the default:

```
device(config)# no system-monitor-mail relay 10.70.212.167 domain-name domain_name2.Extreme.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
Type: 1GLR
+------------+-------------------------+-------------------------+--------+
|            |      High Threshold     |      Low Threshold      | Buffer |
| Area       | Value | Above | Below   | Value     | Below       | Value  |
|            |       | Action| Action  |           | Action      |        |
+------------+-------+-------+-------+-----------+------------+--------+
| Temp C     |    90 | raslog| none    |       -45| raslog      |      0|
+------------+-------+-------+-------+-----------+------------+--------+
| RXP uWatts |   501 | raslog| none    |         6| raslog      |      0|
+------------+-------+-------+-------+-----------+------------+--------+
| TXP uWatts |   794 | raslog| none    |        71| raslog      |      0|
+------------+-------+-------+-------+-----------+------------+--------+
| Current mA |    45 | raslog| none    |         1| raslog      |      0|
+------------+-------+-------+-------+-----------+------------+--------+
| Voltage mV |  3700 | raslog| none    |      2900| raslog      |      0|
+------------+-------+-------+-------+-----------+------------+--------+
device#
```

Viewing the area-wise optical monitoring current status

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

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

Displaying the device health status

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

```
device# show system monitor
** System Monitor Switch Health Report **
                    Switch status          : HEALTHY
                    Time of Report         : 2017-03-10 06:33:27
                    Power supplies monitor  : HEALTHY
                    Temperatures monitor   : HEALTHY
                    Fans monitor           : HEALTHY
                    Flash monitor          : HEALTHY
device#
```

Logging and tracing

Overview

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

RASTrace captures low level info which can be used for debugging or troubleshooting issues. Use the **rasdecode** command to decode the traces collected. You must provide the module ID (–m) and display count (–n) parameters.

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

RASLog

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

It can store 2048 external customer visible messages in total. These are forwarded to the console, to the configured syslog servers and through the SNMP traps or informs the SNMP management station.

There are four levels of severity for messages, ranging from CRITICAL to INFO. In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. You must look at each specific error message description thoroughly before taking action.

TABLE 2 Severity levels of the RASLog messages

Severity level	Description
CRITICAL	Critical-level messages indicate that the software has detected serious problems that cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
ERROR	Error-level messages represent an error condition that does not affect overall system functionality significantly. For example, error-level messages may indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
WARNING	Warning-level messages highlight a current operating condition that must be checked or it may lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
INFO	Info-level messages report the current non-error status of the system components; for example, detecting online and offline status of an interface.

For more information on RASLog messages, refer the *Extreme SLX-OS Message Reference*.

AuditLog

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

DCMCFG audits all the configuration changes in DB. FIRMWARE audit the events occurring during firmware download process. SECURITY audit any user-initiated security event for all management interfaces. Audit log messages are saved in the persistent storage. The storage has a limit of 1024 entries and will wrap around if the number of messages exceed the limit.

The SLX device can be configured to stream Audit messages to the specified syslog servers. Audit log messages are not forwarded to SNMP management stations.

Following are few sample outputs.

```
device(config)# sflow polling-interval 25
2016/06/02-08:48:39, [SFLO-1004], 1067, M1 | Active | DCE, INFO,
MMVM, Global sFlow polling interval is changed to 25.
2016/06/02-08:48:39, [SFLO-1006], 1068, M1 | Active | DCE, INFO,
MMVM, sFlow polling interval on port Ethernet 1/14 is changed to
25.

device# show logging auditlog reverse count 2
394 AUDIT,2016/06/02-08:48:39 (GMT), [DCM-1006], INFO, DCMCFG,
admin/admin/127.0.0.1/console/cli,, SLX9140-4, Event: database
commit transaction, Status: Succeeded, User command: "configure
config sflow polling-interval 25".
393 AUDIT,2016/06/02-08:40:57 (GMT), [SEC-3022], INFO, SECURITY,
root/root/172.22.224.196/telnet/CLI,, MMVM, Event: logout, Status:
success, Info: Successful logout by user [root].
```

For more information on AuditLog messages, refer to the *Extreme SLX-OS Message Reference* for the SLX 9140 and 9240 Switches.

Syslog

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

RASLog and AuditLog infrastructure makes use of Syslog service running on the SLX device to log messages into the local file system or to remote syslog server. All external RASLog messages and all Audit logs are sent to syslog server. SLX-OS uses **syslog-ng** which is an open source implementation of the syslog protocol for Unix and Unix-like systems. It runs over any of the following:

- UDP (default port 514)
- TLS (default port 6514)

A maximum of 4 syslog servers can be configured on any SLX device. These servers can have IPV4 or IPV6 address and reside in mgmt-vrf, default-vrf or user defined VRF. The **logging syslog-server** command enables the syslog event capturing on the syslog server. The IP address, VRF-name and port are the parameters used.

Following are sample syslog events captured at the syslog server.

```
There is no reference to MMVM in Davinci. It's been changed to "SLX".

Please see the example below
=====================
Feb 15 18:10:11 10.24.71.121 SLX raslogd: [log@1588
value="RASLOG"][timestamp@1588 value="2017-02-15T18:10:11.087052"]
msgid@1588 value="NSM-1003"][seqnum@1588 value="1566"][attr@1588
value=" DCE | WWN 10:00:ffffffc4:ffffffff5:7c[severity@1588 value="INFO"]
[swname@1588 value="SLX"][arg0@1588 value="Ethernet 0/1" desc="InterfaceName"]
BOM Interface Ethernet 0/1 is link down.
Feb 15 18:10:11 10.24.71.121 SLX raslogd: [log@1588 value="AUDIT"]
[timestamp@1588 value="2017-02-15T18:10:11.112495"][tz@1588 value="GMT"]
```

```
[msgid@1588 value="DCM-1006"][severity@1588 value="INFO"]
[class@1588 value="DCMCFG"][user@1588 value="admin"][role@1588 value="admin"]
[ip@1588 value="127.0.0.1"][interface@1588 value="console"][application@1588 value="cli"]
[swname@1588 value="SLX9140"][arg0@1588 value="database commit transaction" desc="Event Name"]
[arg1@1588 value="Succeeded" desc="Command status"]
[arg2@1588 value=""configure conf-if-eth-0/1 shutdown"" desc="ConfD hpath string"]
BOMEvent: database commit transaction, Status: Succeeded, User command: "configure conf-if-eth-0/1
shutdown".
Feb 15 18:13:02 10.24.71.121 SLX raslogd: [log@1588 value="RASLOG"]
[timestamp@1588 value="2017-02-15T18:13:02.261680"][msgid@1588 value="NSM-1019"]
[seqnum@1588 value="1567"][attr@1588 value=" DCE | WWN 10:00:ffffffc4:ffffffff5:7c[severity@1588
value="INFO"]
[swname@1588 value="SLX"][arg0@1588 value="Ethernet 0/1" desc="InterfaceName"]
BOM Interface Ethernet 0/1 is administratively up.
Feb 15 18:13:02 10.24.71.121 SLX raslogd: [log@1588 value="AUDIT"]
[timestamp@1588 value="2017-02-15T18:13:02.292919"]
[tz@1588 value="GMT"][msgid@1588 value="DCM-1006"]
[severity@1588 value="INFO"][class@1588 value="DCMCFG"]
[user@1588 value="admin"][role@1588 value="admin"][ip@1588 value="127.0.0.1"]
[interface@1588 value="console"][application@1588 value="cli"]
[swname@1588 value="SLX9140"][arg0@1588 value="database commit transaction" desc="Event Name"]
[arg1@1588 value="Succeeded" desc="Command status"]
[arg2@1588 value=""configure conf-if-eth-0/1 no shutdown"" desc="ConfD hpath string"]
BOMEvent: database commit transaction, Status: Succeeded, User command: "configure conf-if-eth-0/1 no
shutdown".
Feb 15 18:13:03 10.24.71.121 SLX raslogd: [log@1588 value="RASLOG"][timestamp@1588
value="2017-02-15T18:13:03.303235"]
[msgid@1588 value="NSM-1001"][seqnum@1588 value="1568"]
[attr@1588 value=" DCE | WWN 10:00:ffffffc4:ffffffff5:7c[severity@1588 value="INFO"]
[swname@1588 value="SLX"][arg0@1588 value="Ethernet 0/1" desc="InterfaceName"] BOM Interface Ethernet 0/1
is online.
```

For more information on Syslog messages, refer to the *Extreme SLX-OS Message Reference* for the SLX 9140 and SLX 9240 Switches.

.

Importing a syslog CA certificate

The following procedure imports the syslog CA certificate from the remote host to the device.

1. Connect to the device and log in using an account with admin role permissions.

2. In privileged EXEC mode, enter the **certutil import syslogca** command. Include the full path to the certificate on the host, specify SCP as the protocol, and include the IP address of the host.

```
device# certutil import syslogca directory /usr/ldapcacert/ file cacert.pem protocol SCP host 10.23.24.56
user jane password
password: ****
```

Viewing the syslog CA certificate

The following procedure allows you to view the syslog CA certificate that has been imported on the device.

1. Connect to the device and log in using an account with admin role permissions.

2. In privileged EXEC mode, enter the **show cert-util syslogcacert** command.

This example displays the syslog CA certificates.

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

Verifying syslog CA certificates

To test whether a syslog CA certificate has been imported on the device, in privileged EXEC mode, enter the **no certutil syslogca** command and examine the message returned by the system. The command returns an error if there is no syslog CA certificate on the device. If a syslog CA certificate exists on the device, you are prompted to delete it. Enter the **no certutil syslogcacert** command to retain the certificate.

Example for when no syslog CA certificate is present

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

Example for when a syslog CA certificate exists on the device

```
device# no certutil syslogcacert
Do you want to delete syslog CA certificate? [y/n]:n
```

Deleting a syslog CA certificate

The following procedure deletes the syslog CA certificates of all attached Active Directory servers from the device.

1. Connect to the device and log in using an account with admin role permissions.
2. In privileged EXEC mode, enter the **no certutil syslogca** command. You will be prompted to confirm that you want to delete the syslog CA certificates.

This example deletes the syslog CA certificates.

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

sFlow

Overview

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

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

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

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

The sFlow agent uses two forms of operation:

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

sFlow can be port based or ACL based.

In port based sFlow, the sampling entity performs sampling on all flows originating from or destined to a specific port. Each packet is considered only once for sampling, irrespective of the number of ports it is forwarded to. Port based sFlow uses the port level sampling rate, if it is configured. Otherwise, it uses the global sampling rate. When port level sampling rate is unconfigured with 'no' option, it will revert back to using the global sampling rate.

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 based sflow
- VxLAN visibility sflow

Port-based and flow-based sFlow are supported on physical ethernet ports only.

Feature support matrix for sFlow

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

TABLE 3 sFlow feature support

sFlow Feature	Support
sFlow v5	Supported
sFlow MIB	Supported

TABLE 3 sFlow feature support (continued)

sFlow Feature	Support
	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	Filled up with zero.
Agent IP address	Cannot be configured through CLI. Management IP is always used as the Agent IP address.
sFlow source interface	Supports configuration of source interface and corresponding IP of the interface will be the outer source IP of the sflow datagram reaching collector. This is not applicable for sflow packet reaching mgmt-vrf collector.
sFlow counter polling support on per-port, per-VLAN, or per-trunk or per tunnel basis	Supports per-port counter polling only.
Ability to disable sFlow counter polling	Supports global and per-interface level.
AS path cleanup timer (v4: BGP communities, v5: BGP next hop router)	Not 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 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. (Optional) Configure sFlow source-interface.

    ```
    device(config)# sflow source-interface ethernet 0/3
    ```

7. Return to privileged EXEC mode.

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

8. Confirm the sFlow configuration status by using the show sflow or show sflow all commands.

    ```
    device# show sflow
    ```

9. Clear any existing sFlow statistics to ensure accurate readings.

    ```
    device# clear sflow statistics
    ```

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

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

    ```
    device# show running-config sflow
    sflow enable
    sflow source-interface ethernet 0/3
    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
    device# 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 **sflow-profile** command to add an sFlow profile name.

   This example assigns the profile name "profile1."

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

6. Switch to interface configuration mode.

```
device(config-policymap)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)#
```

7. Bind the policy map to an interface.

```
device(conf-if-eth-0/1)# 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 ethernet 0/1
device(conf-if-eth-0/1)#
```

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

```
device(conf-if-eth-0/1)# no service-policy in
```

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

```
device# show sflow interface ethernet 0/1
```

Configuring sFlow for interfaces

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

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

Enabling and customizing sFlow on specific interfaces

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

1. Enter the **interface** command.

```
device(config)# interface ethernet 0/1
```

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

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

3. Configure the sFlow polling interval.

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

4. Set the sFlow sample-rate.

```
device(conf-if-eth-0/1)# 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 ethernet 0/1

sFlow info for interface Ethernet 0/1
-------------------------------------------------
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
Port backoffThreshold :               800
Sflow samples collected:              0
Counter samples collected :           14
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 **sflow-profile**command.

    This example assigns the profile name "profile1"

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

6. Bind the policy map to an interface.

    ```
    switch(conf-if-eth-0/1)# service-policy in policy1
    ```

Disabling sFlow on specific interfaces

> NOTE
> Disabling sFlow on the interface port does not completely shut down the network communication on the interface port.

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

1. Disable the sFlow interface.

    ```
    switch(conf-if-eth-0/1)# no sflow enable
    ```

2. Return to privileged EXEC mode.

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

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

    ```
    switch# show sflow interface interface ethernet 0/1
    ```

Configuration example

Global configuration

```
device(config)# sflow enable
2017/01/23-10:03:34, [SFLO-1001], 4337, DCE, INFO, switch, sFlow is enabled globally.
device(config)# no sflow enable
2017/01/23-10:03:53, [SFLO-1001], 4338, DCE, INFO, switch, sFlow is disabled globally.
device(config)# sflow sample-rate 4096
2017/01/23-10:04:15, [SFLO-1003], 4339, DCE, INFO, switch, Global sFlow sampling rate is changed to 4096.
device(config)# no sflow sample-rate
2017/01/23-10:04:45, [SFLO-1003], 4340, DCE, INFO, switch, Global sFlow sampling rate is changed to 2048.
device(config)# sflow polling-interval 30
2017/01/23-10:05:01, [SFLO-1004], 4341, DCE, INFO, switch, Global sFlow polling interval is changed to 30.
device(config)# no sflow polling-interval
2017/01/23-10:05:19, [SFLO-1004], 4342, DCE, INFO, switch, Global sFlow polling interval is changed to 20.
device(config)# sflow collector 172.22.108.57 6343
2017/01/23-10:06:00, [SFLO-1007], 4343, DCE, INFO, switch, 172.22.108.57 is configured as sFlow collector.
device(config)# sflow collector 10.1.15.2 6343 use-vrf default-vrf
2017/01/23-10:06:47, [SFLO-1007], 4344, DCE, INFO, switch, 10.1.15.2 is configured as sFlow collector.
device(config)# vrf red_vrf
device(config-vrf-red_vrf)# address-family ipv4 unicast
device(vrf-red_vrf-ipv4-unicast)# exit
device(config-vrf-red_vrf)# exit
device(config)# sflow collector 100.1.1.2 6343 use-vrf red_vrf
2017/01/23-10:08:42, [SFLO-1007], 4345, DCE, INFO, switch, 100.1.1.2 is configured as sFlow collector.
device(config)# do show sflow
sFlow services are:                     disabled
Global default sampling rate:           2048 pkts
Global default counter polling interval: 20 secs
Collector server address       Vrf-Name        Sflow datagrams sent
-------------------------------------------------------------------
10.1.15.2:6343                 default-vrf          0
100.1.1.2:6343                 red_vrf              0
172.22.108.57:6343             mgmt-vrf             0

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)# no sflow collector 172.22.108.57
2017/01/23-10:12:38, [SFLO-1007], 4347, DCE, INFO, switch, 172.22.108.57 is unconfigured as sFlow collector.
device(config)# no sflow collector 10.1.15.2 6343 use-vrf default-vrf
2017/01/23-10:13:13, [SFLO-1007], 4348, DCE, INFO, switch, 10.1.15.2 is unconfigured as sFlow collector.
device(config)# no sflow collector 100.1.1.2 6343 use-vrf red_vrf
2017/01/23-10:13:54, [SFLO-1008], 4349, DCE, INFO, switch, All the sFlow collectors are unconfigured.
device(config)#
```

Interface configuration

```
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# sflow enable
2017/01/23-10:22:29, [SFLO-1002], 4351, DCE, INFO, switch, sFlow is enabled for port Ethernet 0/1.
device(conf-if-eth-0/1)# no sflow enable
2017/01/23-10:22:40, [SFLO-1002], 4352, DCE, INFO, switch, sFlow is disabled for port Ethernet 0/1.
device(conf-if-eth-0/1)# sflow enable
2017/01/23-10:23:13, [SFLO-1002], 4353, DCE, INFO, switch, sFlow is enabled for port Ethernet 0/1.
device(conf-if-eth-0/1)# sflow sample-rate 8192
2017/01/23-10:23:24, [SFLO-1005], 4354, DCE, INFO, switch, sFlow sampling rate on port Ethernet 0/1 is
changed to 8192.
device(conf-if-eth-0/1)# no sflow sample-rate
2017/01/23-10:23:34, [SFLO-1005], 4355, DCE, INFO, switch, sFlow sampling rate on port Ethernet 0/1 is
changed to 2048.
device(conf-if-eth-0/1)# sflow polling-interval 40
2017/01/23-10:25:01, [SFLO-1006], 4356, DCE, INFO, switch, sFlow polling interval on port Ethernet 0/1 is
changed to 40.
device(conf-if-eth-0/1)# no sflow polling-interval
2017/01/23-10:25:12, [SFLO-1006], 4357, DCE, INFO, switch, sFlow polling interval on port Ethernet 0/1 is
changed to 20.
device(conf-if-eth-0/1)#
```