S Commands

This chapter describes the system management commands that begin with S.

shut (ERSPAN)

To shut down an Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **shut** command. To enable an ERSPAN session, use the **no** form of this command.

shut

no shut

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

ERSPAN session configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to shut down an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# shut
switch(config-erspan-src)#
```

This example shows how to enable an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# no shut
switch(config-erspan-src)#
```

Related Commands

Command	Description
monitor session	Enters the monitor configuration mode.
show monitor session	Displays the virtual SPAN or ERSPAN configuration.

snmp-server community

To create Simple Network Management Protocol (SNMP) communities for SNMPv1 or SNMPv2c, use the **snmp-server community** command. To revert to the defaults, sue the **no** form of this command.

snmp-server community *com-name* [**group** *grp-name* | **ro** | **rw** | **use-acl** *acl-name*]

no snmp-server community *com-name* [**group** *grp-name* | **ro** | **rw** | **use-acl** *acl-name*]

Syntax Description

com-name	SNMP community string. The name can be any alphanumeric string up to 32 characters.
group *grp-name*	(Optional) Specifies the group to which the community belongs. The name can be a maximum of 32 characters.
ro	(Optional) Specifies read-only access with this community string.
rw	(Optional) Specifies read-write access with this community string.
use-acl *acl-name*	(Optional) Specifies the access control list (ACL) to filter SNMP requests. The name can be a maximum of 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.

See the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide* for more information on creating ACLs. The ACL applies to both IPv4 and IPv6 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community.

Examples

This example shows how to create an SNMP community string and assign an ACL to the community to filter SNMP requests:

```
switch(config)# snmp-server community public use-acl my_acl_for_public
switch(config)#
```

Related Commands

Command	Description
show snmp community	Displays the SNMP community strings.

snmp-server contact

To configure the Simple Network Management Protocol (SNMP) contact (sysContact) information, use the **snmp-server contact** command. To remove the contact information, use the **no** form of this command.

snmp-server contact [*text*]

no snmp-server contact [*text*]

Syntax Description

text	(Optional) String that describes the system contact information. The text can be any alphanumeric string up to 32 characters and cannot contain spaces.

Command Default

No system contact (sysContact) string is set.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to set an SNMP contact:

```
switch(config)# snmp-server contact DialSystemOperatorAtBeeper#1235
switch(config)#
```

This example shows how to remove an SNMP contact:

```
switch(config)# no snmp-server contact DialSystemOperatorAtBeeper#1235
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays information about SNMP.
snmp-server location	Sets the system location string.

snmp-server context

To configure the Simple Network Management Protocol (SNMP) context to logical network entity mapping, use the **snmp-server context** command. To remove the context, use the **no** form of this command.

snmp-server context *context-name* [**instance** *instance-name*] [**vrf** {*vrf-name* | **default** | **management**}] [**topology** *topology-name*]

no snmp-server context *context-name* [**instance** *instance-name*] [**vrf** {*vrf-name* | **default** | **management**}] [**topology** *topology-name*]

Syntax Description

context-name	SNMP context. The name can be any alphanumeric string up to 32 characters.
instance *instance-name*	(Optional) Specifies a protocol instance. The name can be any alphanumeric string up to 32 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name is case sensitive, and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.
topology *topology-name*	(Optional) Specifies the topology. The name can be any alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the **snmp-server context** command to map between SNMP contexts and logical network entities, such as protocol instances or VRFs.

Examples

This example shows how to map the public1 context to the default VRF:

```
switch(config)# snmp-server context public1 vrf default
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays the SNMP status.
show snmp context	Displays information about SNMP contexts.

snmp-server enable traps

To enable the Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps** command. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps
[**aaa** [**server-state-change**] |
callhome [**event-notify** | **smtp-send-fail**] |
entity {**entity_fan_status_change** | **entity_mib_change** | **entity_module_inserted** |
entity_module_removed | **entity_module_status_change** | **entity_power_out_change** |
entity_power_status_change | **entity_unrecognised_module**} |
fcdomain |
fcns |
fcs |
fctrace |
fspf |
license [**notify-license-expiry** | **notify-license-expiry-warning** | **notify-licensefile-missing** |
notify-no-license-for-feature] |
link |
rf [**redundancy_framework**] |
rmon [**fallingAlarm** | **hcFallingAlarm** | **hcRisingAlarm** | **risingAlarm**] |
rscn |
snmp [**authentication**] |
vsan | **vtp** |
zone [**default-zone-behavior-change** | **merge-failure** | **merge-success** | **request-reject1** |
unsupp-mem]]

no snmp-server enable traps
[**aaa** [**server-state-change**] |
callhome [**event-notify** | **smtp-send-fail**] |
entity {**entity_fan_status_change** | **entity_mib_change** | **entity_module_inserted** |
entity_module_removed | **entity_module_status_change** | **entity_power_out_change** |
entity_power_status_change | **entity_unrecognised_module**} |
fcdomain |
fcns |
fcs |
fctrace |
fspf |
license [**notify-license-expiry** | **notify-license-expiry-warning** | **notify-licensefile-missing** |
notify-no-license-for-feature] |
link |
rf [**redundancy_framework**] |
rmon [**fallingAlarm** | **hcFallingAlarm** | **hcRisingAlarm** | **risingAlarm**] |
rscn |
snmp [**authentication**] |
vsan | **vtp** |
zone [**default-zone-behavior-change** | **merge-failure** | **merge-success** | **request-reject1** |
unsupp-mem]]

Syntax Description

aaa	(Optional) Enables notifications for a AAA server state change.
server-state-change	(Optional) Specifies the AAA server state change.

callhome	(Optional) Enables Cisco Call Home notifications.
event-notify	(Optional) Specifies the Cisco Call Home external event notification.
smtp-send-fail	(Optional) Specifies the SMTP message send fail notification.
entity	(Optional) Enables notifications for a change in the module status, fan status, or power status.
entity_fan_status_ change	(Optional) Specifies the entity fan status change.
entity_mib_change	(Optional) Specifies the entity MIB change.
entity_module_ inserted	(Optional) Specifies the entity module inserted.
entity_module_ removed	(Optional) Specifies the entity module removed.
entity_module_status_ change	(Optional) Specifies the entity module status change.
entity_power_out_ change	(Optional) Specifies the entity power out change.
entity_power_status_ change	(Optional) Specifies the entity power status change.
entity_unrecognised_ module	(Optional) Specifies the entity unrecognized module.
fcdomain	(Optional) Enables notifications for the Fibre Channel domain.
fcns	(Optional) Enables notifications for the name server.
fcs	(Optional) Enables notifications for the fabric configuration server.
fctrace	(Optional) Enables notifications for the route to an N port.
fspf	(Optional) Enables notifications for the Fabric Shortest Path First (FSPF).
license	(Optional) Enables notifications for the license manager.
notify-license-expiry	(Optional) Specifies the license expiry notification.
notify-license-expiry-warning	(Optional) Specifies the license expiry warning notification.
notify-licensefile-missing	(Optional) Specifies the license file missing notification.
notify-no-license-for-feature	(Optional) Specifies that a notification is sent when no license needs to be installed for the feature.
link	(Optional) Enables notifications for uplink and downlink interfaces.
rf	(Optional) Enables notifications for the redundancy framework.
redundancy_ framework	(Optional) Specifies the Redundancy_Framework (RF) supervisor switchover MIB.
rmon	(Optional) Enables notifications for rising, falling, and high-capacity alarms.
fallingAlarm	(Optional) Specifies the RMON falling alarm.
hcFallingAlarm	(Optional) Specifies the high-capacity RMON falling alarm.
hcRisingAlarm	(Optional) Specifies the high-capacity RMON rising alarm.
risingAlarm	(Optional) Specifies the RMON rising alarm.
rscn	(Optional) Enables RSCN notifications.

snmp	(Optional) Enables SNMP authentication notifications.
authentication	(Optional) Specifies the SNMP authentication trap.
vsan	(Optional) Enables notifications for VSANs.
vtp	(Optional) Enables notifications for a VLAN Trunking Protocol (VTP) domain.
zone	(Optional) Enables zone notifications.
default-zone-behavior-change	(Optional) Specifies the default zone behavior change notification.
merge-failure	(Optional) Specifies the merge failure notification.
merge-success	(Optional) Specifies the merge success notification.
request-reject1	(Optional) Specifies the request reject notification.
unsupp-mem	(Optional) Specifies the unsupported member notification.

Command Default

All notifications

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

The **snmp-server enable traps** command enables both traps and informs, depending on the configured notification host receivers.

Examples

This example shows how to enable SNMP notifications for the server state change:

```
switch(config)# snmp-server enable traps aaa
switch(config)#
```

This example shows how to disable all SNMP notifications:

```
switch(config)# no snmp-server enable traps
switch(config)#
```

Related Commands

Command	Description
snmp-server enable traps link	Enables the Simple Network Management Protocol (SNMP) notifications on link traps.
show snmp trap	Displays the SNMP notifications enabled or disabled.

snmp-server enable traps link

To enable the Simple Network Management Protocol (SNMP) notifications on link traps, use the **snmp-server enable traps link** command. To disable SNMP notifications on link traps, use the **no** form of this command.

snmp-server enable traps link [*notification-type*]

no snmp-server enable traps link [*notification-type*]

Syntax Description

notification-type	(Optional) Type of notification to enable. If no type is specified, all notifications available on your device are sent. The notification type can be one of the following keywords: • **IETF-extended-linkDown**—Enables the Internet Engineering Task Force (IETF) extended link state down notification. • **IETF-extended-linkUp**—Enables the IETF extended link state up notification. • **cisco-extended-linkDown**—Enables the Cisco extended link state down notification. • **cisco-extended-linkUp**—Enables the Cisco extended link state up notification. • **connUnitPortStatusChange**—Enables the overall status of the connectivity unit Notification. • **delayed-link-state-change**—Enables the delayed link state change. • **fcTrunkIfDownNotify**—Enables the Fibre Channel Fabric Element (FCFE) link state down notification. • **fcTrunkIfUpNotify**—Enables the FCFE link state up notification. • **fcot-inserted**—Specifies that the Fibre Channel optical transmitter (FCOT) hardware has been inserted. • **fcot-removed**—Specifies that the FCOT has been removed. • **linkDown**—Enables the IETF Link state down notification. • **linkUp**—Enables the IETF Link state up notification.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This command is disabled by default. Most notification types are disabled.

If you enter this command with no *notification-type* arguments, the default is to enable all notification types controlled by this command

Examples

This example shows how to enable the SNMP link trap notification on the switch:

```
switch(config)# snmp-server enable traps link
switch(config)#
```

This example shows how to disable the SNMP link trap notification on the switch:

```
switch(config)# no snmp-server enable traps link
switch(config)#
```

Related Commands

Command	Description
show snmp trap	Displays the SNMP notifications enabled or disabled.

snmp-server globalEnforcePriv

To configure Simple Network Management Protocol (SNMP) message encryption for all users, use the **snmp-server globalEnforcePriv** command. To remove the encryption, use the **no** form of this command.

snmp-server globalEnforcePriv

no snmp-server globalEnforcePriv

Syntax Description

This command has no arguments or keywords.

Command Default

The SNMP agent accepts SNMPv3 messages without authentication and encryption.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to configure SNMP message encryption for all users:

```
switch(config)# snmp-server globalEnforcePriv
switch(config)#
```

This example shows how to remove SNMP message encryption for all users:

```
switch(config)# no snmp-server globalEnforcePriv
switch(config)#
```

Related Commands

Command	Description
snmp-server user	Configures a new user to an SNMP group.
show snmp sessions	Displays the current SNMP sessions.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command. To remove the specified host, use the **no** form of this command.

snmp-server host *host-address* {*community-string*
| filter-vrf {*vrf-name* | **default** | **management**}
| {informs | traps} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}
community-string [**udp-port** *port*]}
| version {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* [**udp-port** *port*]}

no snmp-server host *host-address* {*community-string*
| filter-vrf {*vrf-name* | **default** | **management**}
| {informs | traps} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}
community-string [**udp-port** *port*]}
| version {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* [**udp-port** *port*]}

Syntax Description

host-address	IPv4 or IPv6 address or DNS name of the SNMP notification host.
community-string	String sent with the notification operation. The string can be a maximum of 32 alphanumeric characters. We recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
filter-vrf *vrf-name*	Specifies the virtual routing and forwarding (VRF) instance. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.
informs	Sends SNMP informs to this host.
traps	Sends SNMP traps to this host.
version	Specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following must be specified: • **1**—SNMPv1. • **2c**—SNMPv2C. • **3**—SNMPv3. The following three optional keywords can follow the **version 3** keyword: – **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – **noauth** (Default)—The noAuthNoPriv security level. This is the default if the **auth**, **noauth**, or **priv** keyword is not specified. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”)
udp-port *port*	(Optional) Specifies the UDP port of the host to use. The port range is from 0 to 65535.

Command Default Disabled

Command Modes Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Therefore, informs are more likely to reach their intended destination.

Examples This example shows how to sends the SNMP traps to the host specified by the IPv4 address 192.168.0.10. The community string is defined as my_acl_for_public.:

```
switch(config)# snmp-server community public use-acl my_acl_for_public
switch(config)# snmp-server host 192.168.0.10 my_acl_for_public
switch(config)#
```

This example shows how to send all inform requests to the host myhost.cisco.com using the community string my_acl_for_public:

```
switch(config)# snmp-server enable traps
switch(config)# snmp-server host myhost.cisco.com informs version 2c my_acl_for_public
switch(config)#
```

Related Commands

Command	Description
show snmp host	Displays information about the SNMP host.

snmp-server location

To set the Simple Network Management Protocol (SNMP) system location string, use the **snmp-server location** command. To remove the location string, use the **no** form of this command.

snmp-server location [*text*]

no snmp-server location [*text*]

Syntax Description

text	(Optional) String that describes the system location information.

Command Default

No system location string is set.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to set a system location string:

```
switch(config)# snmp-server location Building 3/Room 21
switch(config)#
```

This example shows how to remove the system location string:

```
switch(config)# no snmp-server location Building 3/Room 21
switch(config)#
```

Related Commands

Command	Description
snmp-server contact	Sets the SNMP system contact (sysContact) string.

snmp-server mib community-map

To configure a Simple Network Management Protocol (SNMP) context to map to a logical network entity, such as a protocol instance or VRF, use the **snmp-server mib community-map** command. To remove the mapping, use the **no** form of this command.

snmp-server mib community-map *community-string* **context** *context-name*

no snmp-server mib community-map *community-string* **context** *context-name*

Syntax Description

community-string	String sent with the notification operation. The string can be a maximum of 32 alphanumeric characters. We recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server mib community-map** command.
context	Specifies the SNMP context to be mapped to the logical network entity.
context-name	SNMP context. The name can be any alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to map an SNMPv2c community named my_acl_for_public to an SNMP context public1:

```
switch(config)# snmp-server mib community-map my_acl_for_public context public1
switch(config)#
```

This example shows how to remove the mapping of an SNMPv2c community to an SNMP context:

```
switch(config)# no snmp-server mib community-map my_acl_for_public context public1
switch(config)#
```

Related Commands

Command	Description
snmp-server community	Configures an SNMP community.
snmp-server context	Configures an SNMP context.
show snmp	Displays the SNMP status.

snmp-server tcp-session

To enable a one-time authentication for Simple Network Management Protocol (SNMP) over a TCP session, use the **snmp-server tcp-session** command. To disable the one-time authentication, use the **no** form of this command.

snmp-server tcp-session [**auth**]

no snmp-server tcp-session [**auth**]

Syntax Description

auth	(Optional) Specifies that one-time authentication for SNMP be enabled over the TCP session.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to enable one-time authentication for SNMP over a TCP session:

```
switch(config)# snmp-server tcp-session auth
switch(config)#
```

This example shows how to disable one-time authentication for SNMP over a TCP session:

```
switch(config)# no snmp-server tcp-session auth
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays the SNMP status.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username* [*groupname*] [**auth** {**md5** | **sha**} *auth-password* [{**engineID** *engine-ID* | **localizedkey** | **priv** {*priv-password* | **aes-128**}}]]

no snmp-server user

Syntax Description

username	Name of the user on the host that connects to the agent. The name can be a maximum of 32 alphanumeric characters.
groupname	(Optional) Name of the group to which the user is associated. The name can be a maximum of 32 alphanumeric characters.
auth	(Optional) Specifies that an authentication level setting will be initiated for the session.
md5	(Optional) Specifies that the HMAC-MD5-96 authentication level be used for the session.
sha	(Optional) Specifies that the HMAC-SHA-96 authentication level be used for the session.
auth-password	(Optional) Authentication password for the user that enables the agent to receive packets from the host. The password can be a maximum of 130 characters.
engineID *engine-ID*	(Optional) Specifies the SNMP engine ID.
localizedkey	(Optional) Specifies whether the passwords are in localized key format.
priv	(Optional) The option that initiates a privacy authentication level setting session.
priv-password	(Optional) Privacy password for the user that enables the host to encrypt the content of the message that it sends to the agent. The password can be a maximum of 130 characters.
aes-128	(Optional) Specifies that a 128-bit AES algorithm for privacy be used for the session.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to configure an SNMP user named authuser with authentication and privacy parameters:

```
switch(config)# snmp-server user authuser publicsecurity auth sha shapwd priv aes-128
switch(config)#
```

This example shows how to delete an SNMP user:

```
switch(config)# no snmp-server user authuser
switch(config)#
```

Related Commands

Command	Description
show snmp user	Displays information about one or more SNMP users.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation on an interface, use the **snmp trap link-status** command. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status

no snmp trap link-status

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration mode
Virtual Ethernet interface configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

By default, SNMP link traps are sent when a Layer 2 interface goes up or down. You can disable SNMP link trap notifications on an individual interface. You can use these limit notifications on a flapping interface (an interface that transitions between up and down repeatedly).

You can use this command on the following interfaces:

- Layer 2 interface
- Layer 3 interface

Note Use the **no switchport** command to configure an interface as a Layer 3 interface.

- Virtual Ethernet interface

Examples

This example shows how to disable SNMP link-state traps for a specific Layer 2 interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# no snmp trap link-status
switch(config-if)#
```

This example shows how to enable SNMP link-state traps for a specific Layer 3 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# snmp trap link-status
switch(config-if)#
```

This example shows how to enable SNMP link-state traps for a specific Layer 2 interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# snmp trap link-status
switch(config-if)#
```

This example shows how to enable SNMP link-state traps for a specific virtual Ethernet interface:

```
switch(config)# interface vethernet 1
switch(config-if)# snmp trap link-status
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
no switchport	Configures an interface as a Layer 3 routed interface.
show snmp trap	Displays the SNMP notifications, enabled or disabled.

source (SPAN, ERSPAN)

To add an Ethernet Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) source port, use the **source** command. To remove the source SPAN or ERSPAN port, use the **no** form of this command.

source {**interface** {**ethernet** *slot*/[*QSFP-module/*]*port* | **port-channel** *channel-num* | **vethernet** *veth-num*} [{**both** | **rx** | **tx**}] | **vlan** *vlan-num* | **vsan** *vsan-num*}

no source {**interface** {**ethernet** *slot*/[*QSFP-module/*]*port* | **port-channel** *channel-num* | **vethernet** *veth-num*} | **vlan** *vlan-num* | **vsan** *vsan-num*}

Syntax Description

interface	Specifies the interface type to use as the source SPAN port.
ethernet *slot*/[*QSFP-module/*]*port*	Specifies the Ethernet interface to use as the source SPAN port. The slot number is from 1 to 255. The *QSFP-module* number is from 1 to 4. The port number is from 1 to 128. **Note** The *QSFP-module* number applies only to the QSFP+ Generic Expansion Module (GEM).
port-channel *channel-num*	Specifies the EtherChannel interface to use as the source SPAN port. The EtherChannel number is from 1 to 4096.
vethernet *veth-num*	Specifies the virtual Ethernet interface to use as the source SPAN or ERSPAN port. The virtual Ethernet interface number is from 1 to 1048575.
both	(Optional) Specifies both ingress and egress traffic on the source port. **Note** This keyword applies to the ERSPAN source port.
rx	(Optional)Specifies only ingress traffic on the source port. **Note** This keyword applies to the ERSPAN source port.
tx	(Optional) Specifies only egress traffic on the source port. **Note** This keyword applies to the ERSPAN source port.
vlan *vlan-num*	Specifies the VLAN inteface to use as the source SPAN port. The range is from 1 to 3967 and 4048 to 4093.
vsan *vsan-num*	Specifies the virtual storage area network (VSAN) to use as the source SPAN port. The range is from 1 to 4093.

Command Default

None

Command Modes

SPAN session configuration mode
ERSPAN session configuration mode

Command History

Release	Modification
6.0(2)N1(2)	Support for the QSFP+ GEM was added.
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

A source port (also called a *monitored port*) is a switched port that you monitor for network traffic analysis. In a single local SPAN session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both).

A source port can be an Ethernet port, port channel, SAN port channel, VLAN, or a VSAN port. It cannot be a destination port.

For ERSPAN, if you do not specify **both**, **rx**, or **tx**, the source traffic is analyzed for both directions.

Examples

This example shows how to configure an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 9 type local
switch(config-monitor)# description A Local SPAN session
switch(config-monitor)# source interface ethernet 1/1
switch(config-monitor)#
```

This example shows how to configure a port channel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 5
switch(config-monitor)#
```

This example shows how to configure an ERSPAN source port to receive traffic on the port:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# source interface ethernet 1/5 rx
switch(config-erspan-src)#
```

Related Commands

Command	Description
destination (SPAN, ERSPAN)	Configures a destination SPAN port.
monitor session	Creates a new SPAN session configuration.
show monitor session	Displays SPAN session configuration information.
show running-config monitor	Displays the running configuration information of a SPAN session.

switchport monitor rate-limit

To configure a rate limit to monitor traffic on an interface, use the **switchport monitor rate-limit** command. To remove a rate limit, use the **no** form of this command.

switchport monitor rate-limit 1G

no switchport monitor rate-limit [**1G**]

Syntax Description

1G	(Optional) Specifies that the rate limit is 1 GB.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This command is applicable to the following Cisco Nexus 5000 Series switches:

- Cisco Nexus 5010 Series
- Cisco Nexus 5020 Series

This command does not require a license.

Examples

This example shows how to limit the bandwidth on Ethernet interface 1/2 to 1 GB:

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport monitor rate-limit 1G
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport private-vlan association trunk	Associates the isolated trunk port with the primary and secondary VLANs of a private VLAN.

switch-profile

To create or configure a switch profile, use the **switch-profile** command. To delete a switch profile, use the **no** form of this command.

switch-profile *sw-profile-name*

no switch-profile *sw-profile-name* {**all-config | local-config | profile-only**}

Syntax Description

sw-profile-name	Name of the switch profile. The name is case sensitive, can be a maximum of 64 alphanumeric characters and can include an underscore and hyphen. The name cannot contain spaces or special characters.
all-config	Specifies that the switch profile be deleted with all local and peer configurations.
local-config	Specifies that the switch profile and all local configurations be deleted.
profile-only	Specifies that the switch profile only is to be deleted and no other configurations.

Command Default

None

Command Modes

Configuration synchronization mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use this command to create a switch profile on each of the peer switches. You must use the same profile name on both the switches in the Cisco Fabric Services (CFS) peer configuration.

You can configure only one active switch profile on each peer switch. If you create or configure a second switch profile, you see the following error message:

```
Error: Another switch profile already exists. Cannot configure more than one
switch-profile.
```

The configuration that is made locally on the switch is synchronized and made available on the peer switch only after the connectivity is established between the peer switches and the configuration is verified and committed on the local switch.

You can configure a switch profile to include the interface configuration, quality of service (QoS), and virtual port channel (vPC) commands. FCoE commands are not supported on a switch profile.

When you delete a switch profile, you can choose to delete the local switch profile with the local configurations on the switch, delete the switch profile with the local configurations and configuration information in the peer, or delete the switch profile only while saving all other configuraiton information. The peer becomes unreachable.

Examples

This example shows how to create a switch profile named s5010 on switch 1 of the peer:

Peer A

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# exit
switch# config sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

This example shows how to create a switch profile named s5010 on switch 2 of the peer:

Peer B

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# exit
switch# config sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

This example shows how to delete a switch profile named s5010 and its local configuration on switch 1 of the peer:

Peer A

```
switch# config sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# no switch-profile s5010 local-config
switch(config-sync)#
```

Related Commands

Command	Description
config sync	Enters configuration synchronization mode.
show switch-profile	Displays the switch profile created on the switch and its configuration revision.
sync-peers destination	Configures the peer switch for configuration synchronization.