



S Commands

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

sampler

To define a sampler and enter the sampler configuration mode, use the **sampler** command. To remove the sampler definition, use the **no** form of this command.

sampler *name*

no sampler *name*

Syntax Description

<i>name</i>	Name of the sampler. The name can have a maximum of 63 alphanumeric characters.
-------------	---

Defaults

No samplers are defined.

Command Modes

Global configuration mode

Command History

Release	Modification
7.0(0)N1(1)	This command was introduced.

Usage Guidelines

NetFlow sampling means that M out of N packets are sampled. When a packet is sampled and there is a NetFlow cache miss, a NetFlow cache entry is created for this flow. The first packet timestamp is updated and the statistics for the first packet are initialized (for example, the bytes are set to the number of bytes in the packet and the packet count is set to one). If there is a NetFlow cache hit when the packet is sampled, the cache for this flow is updated, which includes adding the number of bytes in the packet to the byte counter and incrementing the packet count by one.

Once you enter the **sampler** *name* command, you enter the sampler configuration mode, and the prompt changes to the following:

```
switch(config-flow-sampler)#
```

Within the sampler configuration mode, the following keywords and arguments are available to configure the flow monitor:

- **description** *description*—Provides a description for this sampler; you can add a maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **mode** *sample-num out-of packets*—Configures the sampler mode. The valid values are as follows:
 - *sample-num*—Number of samples per sampling. The range is from 1 to 64.
 - **out-of**—Specifies the samples per packet ratio.
 - *packets*—Number of packets in each sampling. The range is from 1 to 65536, and must be a power of 2.
- **no**—Negates a command or sets its defaults.

This command does not require a license.

Examples

This example shows how to define a sampler and enter the sampler configuration mode:

```
switch(config)# sampler testsampler  
switch(config-flow-sampler)#
```

This example shows how to configure the sampler mode:

```
switch(config)# sampler testsampler  
switch(config-flow-sampler)# mode 24 out-of 1024
```

This example shows how to remove a sampler definition:

```
switch(config)# no sampler testsampler  
switch(config-flow)#
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.
flow record	Creates a flow record.

shut (SPAN, ERSPAN)

To shut down an Ethernet Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **shut** command. To enable a SPAN or 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

- SPAN session configuration mode (config-monitor)
- ERSPAN source session configuration mode (config-erspan-src)
- ERSPAN destination session configuration mode (config-erspan-dst)
- SPAN-on-Drop session configuration mode (config-span-on-drop)
- SPAN-on-Drop ERSPAN session configuration mode (config-span-on-drop-erspan)
- SPAN-on-Latency session configuration mode (config-span-on-latency)
- SPAN-on-Latency ERSPAN session configuration mode (config-span-on-latency-erspan)

Command History	Release	Modification
	7.0(0)N1(1)	This command was modified. This command was implemented in the following modes: SPAN session configuration mode, ERSPAN destination session configuration mode, SPAN-on-Drop session configuration mode, SPAN-on-Drop ERSPAN session configuration mode, SPAN-on-Latency session configuration mode, and SPAN-on-Latency ERSPAN session configuration mode.
	6.0(2)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 source 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 destination session:

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

This example shows how to shut down a SPAN-on-Drop ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type span-on-drop-erspan
switch(config-span-on-drop-erspan)# shut
switch(config-span-on-drop-erspan)#
```

This example shows how to enable a SPAN-on-Latency ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type span-on-latency-erspan
switch(config-span-on-latency-erspan)# no shut
switch(config-span-on-latency-erspan)#
```

This example shows how to shut down a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type local
switch(config-monitor)# shut
switch(config-monitor)#
```

This example shows how to shut down a SPAN-on-Drop session:

```
switch# configure terminal
switch(config)# monitor session 1 type span-on-drop
switch(config-span-on-drop)# shut
switch(config-span-on-drop)#
```

This example shows how to enable a SPAN-on-Latency session:

```
switch# configure terminal
switch(config)# monitor session 1 type span-on-latency
switch(config-span-on-latency)# no shut
switch(config-span-on-latency)#
```

Related Commands

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

sleep instance

To delay the execution of a command by a specified number of seconds in the maintenance profile, use the **sleep instance** command. You can delay multiple instances of a command. To remove the delay, use the **no** form of this command.

sleep instance *instance-number seconds*

no sleep instance *instance-number seconds*

Syntax Description

<i>instance-number</i>	Provides a label for the configuration by specifying a particular instance number. The range is from 0 to 2177483647.
<i>seconds</i>	Specifies the number of seconds by which the execution of the command has to be delayed. The range is from 0 to 2177483647.

Defaults

None

Command Modes

maintenance profile configuration (config-mm-profile)

Command History

Release	Modification
7.3(0)N1(1)	This command was introduced.

Examples

This example shows how to delay the execution of one command by 20 seconds and another command by 10 seconds:

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 200
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-deny
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
```

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
show run mmode	Displays the currently running maintenance profile configuration on a switch.
show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.

snapshot create

To create a snapshot, use the **snapshot create** command.

snapshot create *name description*

Syntax Description

<i>name</i>	The <i>name</i> variable can be 64 characters in length.
<i>description</i>	The <i>description</i> variable can be 256 characters in length.

Defaults

None.

Command History

Release	Modification
7.1.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create a snapshot:

```
switch# snapshot create snap1 For documentation purposes.
Executing show interface... Done
Executing show bgp sessions vrf all... Done
Executing show ip eigrp topology summary... Done
Executing show ipv6 eigrp topology summary... Done
Executing show vpc... Done
Executing show ip ospf vrf all... Done
Feature 'ospfv3' not enabled, skipping...
Executing show isis vrf all... Done
Snapshot 'snap1' created
switch#
```

Related Commands

Command	Description
show snapshots <i>before-maintenance-mode description</i>	Displays snapshots present on the switch.
snapshot delete	Deletes the snapshot.
show snapshot compare	Compares snapshots and showing the summary and details of each feature.

snapshot delete

To delete a single snapshot or to delete all the snapshots in a system, use the **snapshot delete** command.

```
snapshot delete {all | snapshot-name}
```

Syntax Description	all	Deletes all the snapshots in the system.
	<i>snapshot-name</i>	Deletes the specified snapshot.

Defaults	None
----------	------

Command History	Release	Modification
	7.3(0)N1(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples This example shows how to delete all the snapshots in a system:

```
switch# snapshot delete all
```

This example shows how to delete a specific snapshot:

```
switch # snapshot delete snapshot1
```

Related Commands	Command	Description
	show snapshots	Displays snapshots present on the switch.
	snapshot create	Generates a snapshot.
	snapshot section	Adds or deletes a snapshot section.

snapshot section

To add or delete a snapshot section, use the **snapshot section** command.

```
snapshot section {add section "show-command" row-id element-key1 [element-key2] | delete
section}
```

Syntax Description	Parameter	Description
	add	Adds the specified snapshot section to the snapshot.
	<i>section</i>	Names the snapshot section that is added to the snapshot to display the show command output.
	<i>"show command"</i>	Specifies the show command. The output of this show command is displayed in the new snapshot section created. This show command has to be specified within quotation marks ("show").
	<i>row-id</i>	The row-id argument specifies the tag of each row entry of the show command's XML output.
	<i>element-key1</i>	Specifies the tag used to distinguish among row entries in the show command snapshot section output.
	<i>element-key2</i>	(Optional) Specifies another tag used to distinguish among row entries in the show command snapshot section output.
	delete	Deletes the specified snapshot section from the snapshot.

Defaults

None.

Command History

Release	Modification
7.3(0)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add a snapshot section that displays the output of the **show ip route detail vrf all** command to the snapshot:

```
switch# snapshot section add v4route show "show ip route detail vrf all" ROW_prefix
ipprefix
```

This example shows how to delete a snapshot section from the snapshot:

```
switch# snapshot section delete v4route
```

snmp-server aaa-user cache-timeout

To configure the Simple Network Management Protocol (SNMP) time-out value for synchronized AAA users, use the **snmp-server aaa-user cache-timeout** command. To revert to the default settings, use the **no** form of this command.

snmp-server aaa-user cache-timeout *seconds*

no snmp-server aaa-user cache-timeout *seconds*

Syntax Description	<i>seconds</i>	Timeout value, in seconds. The range is from 1 to 86400. The default value is 3600 seconds.
Command Default	3600 seconds	
Command Modes	Global configuration mode	
Command History	Release	Modification
	7.3(2)N1(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the AAA user synchronization timeout value: <pre>switch(config)# snmp-server aaa-user cache-timeout 6000</pre>	
Related Commands	Command	Description
	show snmp	Displays information about SNMP.

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, use 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

<i>com-name</i>	SNMP community string. The name can be any alphanumeric string up to 32 characters.
group <i>grp-name</i>	(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 <i>acl-name</i>	(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
6.0(2)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 *Security Configuration Guide* for your platform 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	<i>text</i>	(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
	6.0(2)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

<i>context-name</i>	SNMP context. The name can be any alphanumeric string up to 32 characters.
instance <i>instance-name</i>	(Optional) Specifies a protocol instance. The name can be any alphanumeric string up to 32 characters.
vrf <i>vrf-name</i>	(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 <i>topology-name</i>	(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
6.0(2)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.
fdomain	(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-server enable traps

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
	6.0(2)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
6.0(2)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
6.0(2)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

<i>host-address</i>	IPv4 or IPv6 address or DNS name of the SNMP notification host.
<i>community-string</i>	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 <i>vrf-name</i>	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: <ul style="list-style-type: none"> • 1—SNMPv1. • 2c—SNMPv2C. • 3—SNMPv3. The following three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> – 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 <i>port</i>	(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
	6.0(2)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 send 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	<i>text</i> (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
	6.0(2)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

<i>community-string</i>	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.
<i>context-name</i>	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
6.0(2)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
	6.0(2)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

<i>username</i>	Name of the user on the host that connects to the agent. The name can be a maximum of 32 alphanumeric characters.
<i>groupname</i>	(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.
<i>auth-password</i>	(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 <i>engine-ID</i>	(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.
<i>priv-password</i>	(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
6.0(2)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
	6.0(2)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.

soft-reload

To perform a manual soft reload of the switch, use the **soft-reload** command.

soft-reload

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	7.3(2)N1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

If a soft reload that has been triggered by using the **soft-reload** command fails, the switch will not be reloaded. Soft reload can then be attempted again by using the **soft-reload** command after the failures shown have been corrected.

Examples This example shows how to perform a manual soft reload of the switch:

```
switch# soft-reload
```

Related Commands	Command	Description
	show system soft-reload status	Displays the status of the soft reload.
	system soft-reload enable	Enables the switch to perform a soft reload after a process crash.

source

To configure the NetFlow exporter interface to use to reach the NetFlow collector for the configured destination, use the **source** command. To remove the source, use the **no** form of this command.

source *if-type if-number*

no source [*if-type if-number*]

Syntax Description	
<i>if-type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>if-number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Defaults None

Command Modes NetFlow exporter configuration (config-flow-exporter)

Command History	Release	Modification
	7.0(0)N1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to configure the NetFlow exporter source interface:

```
switch(config)# flow exporter Netflow-Exporter-1
switch(config-flow-exporter)# source Ethernet3/11
switch(config-flow-exporter)#
```

This example shows how to remove the Netflow exporter source interface configuration:

```
switch(config-flow-exporter)# no source Ethernet3/11
switch(config-flow-exporter)#
```

Related Commands	Command	Description
	show flow exporter	Displays information about NetFlow exporters.

source interface (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 } [{ both | rx | tx}] | vlan vlan-num | vsan vsan-num }
```

Syntax Description		
interface		Specifies the interface type to use as the source SPAN port.
ethernet <i>slot</i> [/ <i>QSFP-module</i>]/ <i>port</i>		Specifies the Ethernet interface to use as the source SPAN port. The <i>slot</i> number is from 1 to 255. The <i>QSFP-module</i> number is from 1 to 199. The <i>port</i> number is from 1 to 128.
port-channel <i>channel-num</i>		Specifies the EtherChannel interface to use as the source SPAN port. The EtherChannel number is from 1 to 4096.
vethernet <i>veth-num</i>		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.
rx		(Optional) Specifies only ingress traffic on the source port.
tx		(Optional) Specifies only egress traffic on the source port.
vlan <i>vlan-num</i>		Specifies the VLAN interface to use as the source SPAN port. Valid values are from 1 to 3967 and 4048 to 4093. For VLAN span sources only ingress traffic is spanned.
vsan <i>vsan-num</i>		Specifies the virtual storage area network (VSAN) to use as the source SPAN port. The range is from 1 to 4093. For VSAN span sources only ingress traffic is spanned.

Command Default None

Command Modes

- SPAN session configuration mode (config-monitor)
- ERSPAN source session configuration mode (config-erspan-src)
- SPAN-on-Drop session configuration mode (config-span-on-drop)
- SPAN-on-Drop ERSPAN session configuration mode (config-span-on-drop-erspan)
- SPAN-on-Latency session configuration mode (config-span-on-latency)
- SPAN-on-Latency ERSPAN session configuration mode (config-span-on-latency-erspan)

Command History

Release	Modification
7.0(0)N1(1)	This command was modified. This command was implemented in the following modes: SPAN session configuration mode, ERSPAN destination session configuration mode, SPAN-on-Drop session configuration mode, SPAN-on-Drop ERSPAN session configuration mode, SPAN-on-Latency session configuration mode, and SPAN-on-Latency ERSPAN session configuration mode.
6.0(2)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.

**Note**

For VLAN and VSAN span sources only ingress traffic is spanned.

There is no limit to the number of egress SPAN source ports.

SAN Port Channel interfaces can be configured as ingress or egress source ports.

The limit on the number of egress (TX) sources in a monitor session has been lifted.

Port-channel interfaces can be configured as both ingress and egress sources.

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

SPAN on Latency sessions analyze source traffic on TX only, and SPAN on Drop sessions analyze source traffic on RX only. .

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:

```
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.

source ip

To add a source port to an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination session use the **source ip** command, in ERSPAN destination session configuration mode. To remove the source port, use the **no** form of this command.

source ip *ip-address*

no source ip *ip-address*

Syntax Description	<i>ip-address</i>	Specifies the IP address of the source port.
---------------------------	-------------------	--

Command Default	None	
------------------------	------	--

Command Modes	ERSPAN destination session configuration mode (config-erspan-dst)	
----------------------	---	--

Command History	Release	Modification
	7.0(0)N1(1)	This command was introduced..

Usage Guidelines	A source port (also called a <i>monitored port</i>) is a switched port that you monitor for network traffic analysis.
-------------------------	--

Examples	This example shows how to configure an ERSPAN destination session source port:
-----------------	--

```
switch# configure terminal
switch(config)# monitor session 11 type erspan-destination
switch(config-erspan-dst)# source ip 10.1.1.1
switch(config-erspan-dst)#
```

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
	6.0(2)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

<i>sw-profile-name</i>	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
6.0(2)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.



Note

In this release of Cisco NX-OS, only a pair of switches can be configured as a peer.

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 configuration information. The peer becomes unreachable.

Examples

This example shows how to create a switch profile named s6000a 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 s6000a
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

This example shows how to create a switch profile named s6000a 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 s6000a
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

This example shows how to delete a switch profile named s6000a 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 s6000a 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.

system fex-group shutdown

To shutdown a Fabric Extender (FEX) group, use the **system fex-group shutdown** command. To bring up a FEX group, use the **no** form of this command.

system fex-group *name* shutdown

no system fex-group *name* shutdown

Syntax Description	<i>name</i>	Specifies the name of the FEX group.
---------------------------	-------------	--------------------------------------

Command Default	None
------------------------	------

Command Modes	Maintenance profile configuration (config-mm-mode)
----------------------	--

Command History	Release	Modification
	7.3(0)N1(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to shutdown a FEX group:
-----------------	---

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# system fex-group fg1 shutdown
```

This example shows how to bring up a FEX group:

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# no system fex-group fg1 shutdown
```

Related Commands	Command	Description
	configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	show run mmode	Displays the currently running maintenance profile configuration on a switch.
	show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.

system mode maintenance

To put the switch in maintenance mode, use the **system mode maintenance** command. To exit the maintenance mode and return to normal mode, use the **no** form of the command.

system mode maintenance

no system mode maintenance

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration (config)

Command History	Release	Modification
	7.3(0)N1(1)	This command was modified. The default mode for Graceful Insertion and Removal (GIR) is "isolate".
	7.1(0)N1(1)	This command was introduced. The default mode for GIR is "shutdown".

Usage Guidelines In Cisco NX-OS Release 7.1(0)N1(1), the default mode for Graceful Insertion and Removal (GIR) is "shutdown". The switch will use the **shutdown** command to bring down the protocols and shut down the physical ports.

Beginning from Cisco NX-OS Release 7.3(0)N1(1), the default mode for GIR is "isolate". The switch will use the **isolate** command to isolate the protocols from the network. The switch will then be isolated from the network but is not shut down.

This command does not require a license.

Examples This example shows how to put the switch in maintenance mode:

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:
```

```
router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate
```

```
Do you want to continue (y/n)? [no] y
```

```
Generating a snapshot before going into maintenance mode
```

Starting to apply commands...

```
Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate
```

Maintenance mode operation successful.

This example shows how to exit the maintenance mode and return to normal mode:

```
switch# configure terminal
switch(config)# no system mode maintenance
```

Following configuration will be applied:

```
router isis 100
  no isolate
router ospf 100
  no isolate
router bgp 100
  no isolate
```

Do you want to continue (y/n)? [no] y

Starting to apply commands...

```
Applying : router isis 100
Applying :   no isolate
Applying : router ospf 100
Applying :   no isolate
Applying : router bgp 100
Applying :   no isolate
```

Maintenance mode operation successful.

Generating Current Snapshot

Please use 'show snapshots compare before_maintenance after_maintenance' to check the health of the system

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
system mode maintenance always-use-custom-profile	Applies the existing custom maintenance mode profile and prevents creation of auto-generated maintenance mode profile.

Command	Description
system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.
system mode maintenance shutdown	Shuts down all protocols and interfaces except the management interface (by using the shutdown command and not the default isolate command).
system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

system mode maintenance always-use-custom-profile

To apply the existing custom maintenance-mode profile and prevent creation of auto-generated maintenance-mode profile, use the **system mode maintenance always-use-custom-profile** command.

system mode maintenance always-use-custom-profile

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration mode (config)

Command History	Release	Modification
	7.3(0)N1(1)	This command was introduced.

Usage Guidelines The **always-use-custom-profile** option forces the **dont-generate-profile** option to be used even if it has not been specified using the **system mode maintenance** command. You cannot use the “shutdown” option when the **always-use-custom-profile** option is being used.

This command does not require a license.

Examples This example shows how to always apply the existing custom maintenance mode profile and prevent creation of auto-generated maintenance mode profile:

```
switch(config)# system mode maintenance always-use-custom-profile
```

Related Commands	Command	Description
	configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	show run mmode	Displays the currently running maintenance profile configuration on a switch.
	show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.

Command	Description
system mode maintenance shutdown	Shuts down all protocols and interfaces except the management interface (by using the shutdown command and not the default isolate command).
system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

system mode maintenance dont-generate-profile

To prevent the dynamic searching of enabled protocols and put the switch in maintenance mode by executing commands configured in a custom maintenance mode profile, use the **system mode maintenance dont-generate-profile** command. To exit maintenance mode and return to normal mode, use the **no** form of this command.

system mode maintenance dont-generate-profile

no system mode maintenance dont-generate-profile

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration (config)

Command History	Release	Modification
	7.3(0)N1(1)	This command was introduced.

Usage Guidelines. This command does not require a license.

Examples This example shows how to prevent the dynamic searching of enabled protocols and put the switch in maintenance mode by executing commands configured in a custom maintenance mode profile:

```
switch(config)# system mode maintenance dont-generate-profile
```

Following configuration will be applied:

```
router bgp 100
  isolate
  sleep instance 1 10
interface Ethernet1/1
  shutdown
```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

```
Applying : router bgp 100
Applying :   isolate
Applying : sleep instance 1 10
Applying : interface Ethernet1/1
Applying :   shutdown
```

Maintenance mode operation successful.

Related Commands	Command	Description
	configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	show run mmode	Displays the currently running maintenance profile configuration on a switch.
	show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.
	system mode maintenance shutdown	Shuts down all protocols and interfaces except the management interface (by using the shutdown command and not the default isolate command).
	system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

system mode maintenance on-reload reset-reason

To boot the switch into maintenance-mode automatically in the event of a specified system crash, use the **system mode maintenance on-reload reset-reason** command. To prevent the switch from being brought up in maintenance mode in the event of a system crash, use the **no** form of this command.

system mode maintenance on-reload reset-reason *reason*

no system mode maintenance on-reload reset-reason *reason*

Syntax Description

<i>reason</i>	Specifies the reset reason. The reset reasons are as follows: <ul style="list-style-type: none"> • HW_ERROR—Hardware error • SVC_FAILURE—Critical service failure • KERN_FAILURE—Kernel panic • WDOG_TIMEOUT—Watchdog timeout • FATAL_ERROR—Fatal error • MANUAL_RELOAD---Manual reload • MAINTENANCE—Reloads the switch in maintenance mode if the switch was already in maintenance mode before reload. • MATCH_ANY—Any of the above reasons • ANY_OTHER—Any reload reason not specified above
---------------	---

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)N1(1)	This command was introduced.

Usage Guidelines

We recommend configuring the reset reason and saving it to the startup configuration. This enables the switch to go into the maintenance mode after a switch reloads due to any reason.

This command does not require a license.

Examples

This example shows how to automatically boot the switch into maintenance mode if a fatal error or a hardware error occurs

```
switch(config)# system mode maintenance on-reload reset-reason fatal_error
switch(config)# system mode maintenance on-reload reset-reason hw_error
```


Related Commands	Command	Description
	configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	show run mmode	Displays the currently running maintenance profile configuration on a switch.
	show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	system mode maintenance shutdown	Shuts down all protocols and interfaces except the management interface (by using the shutdown command and not the default isolate command).
	system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

system mode maintenance shutdown

To shut down all protocols and interfaces except the management interface (by using the **shutdown** command and not the default **isolate** command), use the **system mode maintenance shutdown** command.

system mode maintenance shutdown

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration (config)

Command History	Release	Modification
	7.3(0)N1(1)	This command was introduced.

Usage Guidelines. This command does not require a license.

Examples This example shows how to shut down all protocol and interfaces on the switch except the management interface:

```
switch# configure terminal
switch(config)# system mode maintenance shutdown
```

Following configuration will be applied:

```
router bgp 100
  shutdown
router ospf 100
  shutdown
router isis 100
  shutdown
system interface shutdown
```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

```
Applying : router bgp 100
Applying : shutdown
Applying : router ospf 100
Applying : shutdown
Applying : router isis 100
Applying : shutdown
Applying : system interface shutdown
```

Maintenance mode operation successful.

Related Commands	Command	Description
	configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	show run mmode	Displays the currently running maintenance profile configuration on a switch.
	show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.
	system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

system mode maintenance timeout

To configure the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes, use the **system mode maintenance timeout** command. To remove the configured timer, use the **no** form of this command.

system mode maintenance timeout *value*

no system mode maintenance timeout *value*

Syntax Description

<i>value</i>	Specifies the number of minutes for which the switch will be in maintenance mode. Range is from 5 to 65535 minutes.
--------------	---

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)N1(1)	This command was introduced.

Usage Guidelines

We recommend setting the timeout value to at least 30 minutes. Once the configured time elapses, the switch returns to normal mode automatically.

This command does not require a license.

Examples

This example shows how to keep the switch in maintenance mode for a specific number of minutes:

```
switch# configure terminal
switch(config)# system mode maintenance timeout 30
```

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
show run mmode	Displays the currently running maintenance profile configuration on a switch.
show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.

system soft-reload enable

To enable the switch to perform a soft reload after a process crash, use the **system soft-reload enable** command. To disable soft reload, use the **no** form of this command.

system soft-reload enable

no system soft-reload enable

Syntax Description This command has no arguments or keywords.

Command Default Soft reload is disabled.

Command Modes Global configuration mode (config)

Command History	Release	Modification
	7.3(2)N1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

A normal switch reload is attempted if a soft reload due to a process crash fails. A soft reload is not triggered when the following scenarios occur:

- If Layer 3 licenses (LAN_BASE_SERVICES_PKG and LAN_ENTERPRISE_SERVICES_PKG) are installed.
- Kernel panic/crash
- Sysmgr crash
- Crashing of the following processes: mmode, provision, xmlma, res, evms, evmc, securityd, aaa, snmpd, callhome, cts, m2rib, stp, ntp, ntpd, bigsurusd, carmelusd, pfma, sensor, pacifica, bootvar, ipqosmgr, vms, sh, libvirtd, init, sysmgr, pfma, vshd, licmgr and sysinfo.

Examples This example shows how to perform a soft reload after a process crash:

```
switch# configure terminal
switch(config)# system soft-reload enable
```

This example shows how to disable soft reload:

```
switch# configure terminal
switch(config)# no system soft-reload enable
```

Related Commands	Command	Description
	show system soft-reload status	Displays the status of the soft reload.
	soft-reload	Performs a manual soft reload of the switch.