Cisco Nexus 3548 Switch NX-OS System Management Command Reference

First Published: April 2013
Last Modified: May 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: OL-27851-02

Cisco Nexus 3548 Switch NX-OS System Management Command Reference

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 3548 Switch NX-OS System Management Command Reference* . It also provides information on how to obtain related documentation.

This preface includes the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco Nexus Series switches.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information that you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for the Cisco Nexus 3000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html

Command References

The command references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_command_reference_list.html

Technical References

The technical references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html

Configuration Guides

The configuration guides are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html

Error and System Messages

The system message reference guide is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3548 Switch NX-OS System Management Command Reference* . The latest version of this document is available at the following Cisco website:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

To check for additional information about this Cisco NX-OS Release, see the *Cisco Nexus 3000 Series Switch Release Notes* available at the following Cisco website:

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

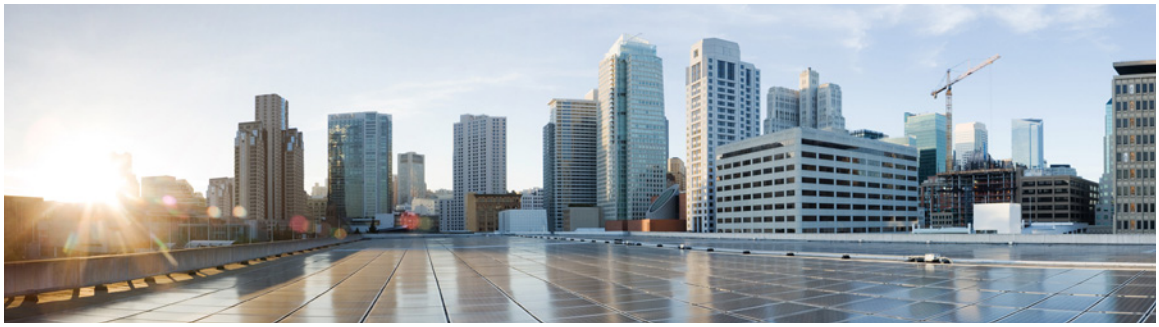
Table 1 summarizes the new and changed features for release 6.x and tells you where they are documented.

Table 1 New and Changed Information for Release 6.x

Feature	Description	Changed in Release	Where Documented
Warp mode	Added support for **hardware profile forwarding-mode normal** and updated options for **hardware profile forwarding-mode warp**.	6.0(2)A8(1)	hardware profile forwarding-mode normal hardware profile forwarding-mode warp
Memory error statistics	Added the command to display the memory error statistics. Added **show logging onboard memory-errors** command output.	6.0(2)A4(6)	show hardware profile buffer monitor summary show logging onboard memory-errors
SPAN and ERSPAN	Added the ability to filter, sample and truncate packets for these features.	6.0(2)A4(1)	filter mtu sampling

Table 1 New and Changed Information for Release 6.x (continued)

Feature	Description	Changed in Release	Where Documented
ERSPAN	This feature was introduced. The **monitor session** command was updated to include the **erspan-destination** and **erspan-source** keywords.	6.0(2)A1(1)	description (SPAN, ERSPAN) destination ip (ERSPAN) destination interface (ERSPAN) monitor erspan origin ip-address monitor session shut (ERSPAN) source (SPAN, ERSPAN) source ip (ERSPAN) vrf (ERSPAN) show monitor session show running-config monitor
Precision Time Protocol (PTP)	This feature was introduced.	6.0(2)A1(1)	clear ptp counters clock protocol feature scheduler ptp announce ptp delay-request minimum interval ptp domain ptp priority1 ptp priority2 ptp source ptp sync interval ptp vlan show ptp brief show ptp clock show ptp clock foreign-masters-record show ptp corrections show ptp parent show ptp port show ptp time-property show scheduler show startup-config ptp



System Management Commands

This chapter describes the Cisco NX-OS system management commands available on the Cisco Nexus 3548 switch.

Note The internal CLI commands are not supported on the Cisco Nexus Series switches.

abort (Call Home)

To discard Call Home configuration changes and release the Cisco Fabric Services (CFS) lock, use the **abort** command.

abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use this command if you are the CFS lock owner or if you are logged into the device that holds the CFS lock.

Examples

This example shows how to discard Call Home configuration changes:

```
switch(config-callhome)# abort
switch(config-callhome)#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

abort (session)

To discard the current configuration session, use the **abort** command.

abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Session configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to abort the current configuration session:

```
switch# configure session MySession1
switch(config-s)# abort
switch#
```

Related Commands

Command	Description
commit	Commits a session.
configure session	Creates a configuration session.
show configuration session	Displays the contents of the session.
verify	Verifies a session.

action cli

To configure a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered, use the **action cli** command. To disable the VSH command string, use the **no** form of this command.

action *label num1* [*.num2*] **cli** [**local**] *vsh_cmd*

no action *label num1* [*.num2*] **cli**

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.
local	(Optional) Specifies the action is to be executed in the same module on which the event occurs.
vsh_cmd	VSH command string to be executed when the applet is triggered.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a VSH command string to be executed when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet cli-applet
switch(config-applet)# action 1.1 cli show version
switch(config-applet)#
```

Related Commands

Command	Description
action counter	Sets or modifies a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.

Command	Description
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

action counter

To set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered, use the **action counter** command. To restore the default value to the counter, use the **no** form of this command.

action *label num1* [*.num2*] **counter name** *name* **value** *value* **op** {**dec** | **inc** | **nop** | **set**}

no action *label num1* [*.num2*] **counter name** *name*

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.
name *name*	Specifies the name of the counter. This identifier can be any string value up to 28 characters.
value *value*	Specifies the value of the counter. This identifier must be an integer value and can be in the range of 0 to 2147483647 or a $-prefixed name (for parameter substitution).
op	Specifies the operation to perform upon the counter.
dec	Decrements the counter by the specified value.
inc	Increments the counter by the specified value.
nop	Does nothing; using this keyword just displays the specified value.
set	Sets the counter to the specified value.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set the counter *count1* to the value in *$variable* when the EEM counter-applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet counter-applet
switch(config-applet)# action 1.2 counter name count1 value $variable op dec
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.
action reload	Specifies the action of reloading the Cisco Nexus 3548 switch software when an Embedded Event Manager (EEM) applet is triggered.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

action event-default

To specify that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered, use the **action event-default** command. To disable the default action, use the **no** form of this command.

action *label num1* [*.num2*] **event-default**

no action *num1* [*.num2*] **event-default**

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the **event-default** statement to the EEM policy or EEM does not allow the CLI command to execute. You can use the **terminal event-manager bypass** command to allow all EEM policies with CLI matches to execute the CLI command.

This command does not require a license.

Examples

This example shows how to specify that the default action for the event is to be performed when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.1 event-default
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.

Command	Description
action policy-default	Enables the default action of the policy being overridden.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

action policy-default

To enable the default action of the policy being overridden, use the **action policy-default** command. To remove the default action, use the **no** form of this command.

action *label num1* [*.num2*] **policy-default**

no action *label num1* [*.num2*] **policy-default**

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the default action of a policy being overridden when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.0 policy-default
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

action reload

To specify the action of reloading the Cisco Nexus 3548 switch software when an Embedded Event Manager (EEM) applet is triggered, use the **action reload** command. To remove the action of reloading the Cisco Nexus 3548 switch software, use the **no** form of this command.

action *label num1* [*.num2*] **reload**

no action *label num1* [*.num2*] **reload**

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the action of reloading the Cisco Nexus 3548 switch software when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet reload-applet
switch(config-applet)# action 1.5 reload
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.

Command	Description
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

action snmp-trap

To specify the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered, use the **action snmp-trap** command. To disable the SNMP trap, use the **no** form of this command.

action *label num1* [*.num2*] **snmp-trap** [**intdata1** *integer*] [**intdata2** *integer*] [**strdata** *string*]

no action *label num1* [*.num2*] **snmp-trap** [**intdata1** *integer*] [**intdata2** *integer*] [**strdata** *string*]

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.
intdata1 *integer*	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent. The *integer* can be any number up to 80 characters.
intdata2 *integer*	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent. The second *integer* can be any number up to 80 characters.
strdata *string*	(Optional) Specifies a string to be sent in the SNMP trap message to the SNMP agent. If the string contains embedded blanks, enclose it in double quotation marks. The *string* can be any alphanumeric string up to 80 characters.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify an SNMP trap to generate when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet snmp-applet
switch(config-applet)# action 1.7 snmp-trap strdata "EEM detected server failure"
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	Sets or modifies a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.
action reload	Specifies the action of reloading the Cisco Nexus 3548 switch software when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

action syslog

To configure a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered, use the **action syslog** command. To disable the syslog message, use the **no** form of this command.

action *label num1* [*.num2*] **syslog** [**priority** {*priority* | *priority-string*}] **msg** *message-text*

no action *label num1* [*.num2*] **syslog** [**priority** {*priority* | *priority-string*}] **msg** *message-text*

Syntax Description

label num1 [*.num2*]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.
priority	(Optional) Specifies the priority level of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level. If this keyword is selected, the priority level argument must be defined.
priority	Priority level as follows: • **emergencies**—Specifies the system is unusable. • **alerts**—Specifies immediate action is needed. • **critical**—Specifies critical conditions. • **errors**—Specifies error conditions. • **warnings**— Specifies warning conditions. • **notifications**—Specifies normal but significant conditions. • **informational**—Specifies informational messages. This is the default. • **debugging**—Specifies debugging messages.
priority-string	$-prefixed parameter that you previously set to a priority level.
msg *message-text*	Specifies the message to be logged. The *message-text* can contain any alphanumeric string up to 256 characters.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Messages written to the syslog from an EEM applet are not screened for EEM syslog events, which might lead to recursive EEM syslog events. Messages that are sent from an EEM applet include the applet name for identification.

This command does not require a license.

Examples

This example shows how to configure a syslog message to save when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet syslog-applet
switch(config-applet)# action 1.7 syslog priority critical msg cpu usage high
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.
action reload	Specifies the action of reloading the Cisco Nexus 3548 switch software when an Embedded Event Manager (EEM) applet is triggered.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.

alert-group (Call Home)

To configure a CLI **show** command for an alert group, use the **alert-group** command. To remove a CLI command from an alert group, use the **no** form of this command.

alert-group *alert* **user-def-cmd** *CLI-command*

no alert-group *alert* **user-def-cmd** *CLI-command*

Syntax Description

alert	Alert group. The *alert* group can be one of the following: • **All**—All alert groups • **Cisco-TAC**—Cisco TAC events • **Configuration**—Configuration events • **Diagnostic**—Diagnostic events • **EEM**—EEM events • **Environmental**—Power, fan, temperature-related events • **Inventory**—Inventory status events • **License**—Licensing events • **Linecard-Hardware**—Linecard-related events • **Supervisor-Hardware**—Supervisor-related events • **Syslog-group-port**—Syslog message events filed by port manager • **System**—Software-related events • **Test**—User-generated test events
user-def-cmd	Specifies a CLI command for an alert group.
CLI-command	CLI **show** command. The command can be a maximum of 512 characters.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can customize predefined alert groups to execute additional CLI **show** commands when specific events occur and send that **show** output with the Call Home message. You can assign a maximum of five user-defined CLI show commands to an alert group.

You must enclose the **show** command in double quotes. Only valid show commands are accepted.

Note You cannot add user-defined CLI **show** commands to the CiscoTAC-1 destination profile.

You can add **show** commands only to full text and XML destination profiles. Short text destination profiles do not support additional **show** commands because they only allow 128 bytes of text.

Examples

This example shows how to add a **show** command output to a Call Home message sent for an alert group:

```
switch(config-callhome)# alert-group configuration user-def-cmd "show running-config"
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome user-def-cmd	Displays information about all user-defined **show** commands added to alert groups.

callhome

To configure the Cisco Smart Call Home service and enter the callhome configuration mode, use the **callhome** command.

callhome

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You must configure the e-mail, phone, and street address information for Call Home. You can optionally configure the contract ID, customer ID, site ID, and switch priority information.

Examples

This example shows how to enter callhome configuration mode:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)#
```

Related Commands

Command	Description
email-contact	Configures the e-mail address.
show callhome	Displays a summary of the Call Home configuration.
snmp-server contact	Configures the SNMP contact (sysContact).

callhome send diagnostic

To send a specified Call Home test message to all configured destinations, use the **callhome send diagnostic** command.

callhome send diagnostic

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can generate a test message to test your Call Home communications using the **callhome send diagnostic** command.

Examples

This example shows how to configure Call Home to send test messages to all configured destinations:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# callhome send diagnostic
switch(config-callhome)#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

callhome test

To send a Call Home test message to all configured destinations, use the **callhome test** command.

callhome test [**inventory**]

Syntax Description

inventory	(Optional) Specifies that a Call Home inventory message be sent for testing the Call Home configuration.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to send a Call Home test message to all configured destinations:

```
switch# callhome test
trying to send test callhome message
successfully sent test callhome message
switch#
```

This example shows how to send a Call Home inventory message to all configured destinations:

```
switch# callhome test inventory
trying to send test callhome inventory message
successfully sent test callhome inventory message
switch#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

clear hardware profile buffer monitor

To clear the buffer monitoring data, use the **clear hardware profile buffer monitor** command.

clear hardware profile buffer monitor

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to clear the buffer monitoring data:

```
switch(config)# clear hardware profile buffer monitor
switch(config)#
```

Related Commands

Command	Description
show hardware buffer monitor	Displays buffer monitoring data.

clear logging logfile

To clears the contents of the log file, use the **clear logging logfile** command.

clear logging logfile

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to clear the logging logfile:

```
switch# clear logging logfile
switch#
```

Related Commands

Command	Description
show logging logfile	Displays the messages in the log file.

clear logging nvram

To clear the NVRAM logs, use the **clear logging nvram** command.

clear logging nvram

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to clear the NVRAM logs:

```
switch# clear logging nvram
switch#
```

Related Commands

Command	Description
show logging nvram	Displays the NVRAM logs.

clear logging onboard

To clear the onboard failure logging (OBFL) entries in the persistent log, use the **clear logging onboard** command.

clear logging onboard [**environmental-history**] [**exception-log**] [**obfl-log**] [**stack-trace**]

Syntax Description

environmental-history	(Optional) Clears the OBFL environmental history.
exception-log	(Optional) Clears the OBFL exception log entries.
obfl-log	(Optional) Clears the OBFL (boot-uptime/device-version/obfl-history).
stack-trace	(Optional) Clears the OBFL stack trace entries.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to clear the OBFL environmental history entries:

```
switch# clear logging onboard environmental-history
switch#
```

This example shows how to clear the OBFL exception-log entries:

```
switch# clear logging onboard exception-log
switch#
```

This example shows how to clear the OBFL (boot-uptime/device-version/obfl-history) entries:

```
switch# clear logging onboard obfl-log
switch#
```

This example shows how to clear the OBFL stack trace entries:

```
switch# clear logging onboard stack-trace
switch#
```

Related Commands

Command	Description
show logging onboard	Displays onboard failure logs.

clear logging session

To clear the current logging session, use the **clear logging session** command.

clear logging session

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to clear the current logging session:

```
switch# clear logging session
switch#
```

Related Commands

Command	Description
show logging session	Displays the logging session status.

clear ntp session

To clear the Network Time Protocol (NTP) session, use the **clear ntp session** command.

clear ntp session

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to discard the NTP Cisco Fabric Services (CFS) distribution session in progress:

```
switch# clear ntp session
switch#
```

Related Commands

Command	Description
show ntp	Displays NTP information.

clear ntp statistics

To clear the Network Time Protocol (NTP) session, use the **clear ntp statistics** command.

clear ntp statistics {**all-peers** | **io** | **local** | **memory**}

Syntax Description

all-peers	Clears all peer transaction statistics.
io	Clears I/O statistics.
local	Clears local statistics.
memory	Clears memory statistics.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to discard the NTP I/O statistics:

```
switch# clear ntp statistics io
switch#
```

Related Commands

Command	Description
show ntp	Displays NTP information.

clear ptp counters

To clear the Precision Time Protocol (PTP) packet counters, use the **clear ptp counters** command.

clear ptp counters {**all** | **interface ethernet** *slot*/*port*}

Syntax Description

all	Clears all PTP counters.
interface	Clears PTP counters from an interface.
ethernet *slot*/*port*	Clears PTP counters from an IEEE 802.3z Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear all PTP counters:

```
switch# clear ptp counters all
switch#
```

Related Commands

Command	Description
feature ptp	Enables PTP on the switch.
show running-config ptp	Displays the PTP running system configuration information.

clear scheduler logfile

To clear the scheduler log file, use the **clear scheduler logfile** command.

clear scheduler logfile

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how clear the scheduler log file:

```
switch# configure terminal
switch(config)# clear scheduler logfile
switch(config)#
```

Related Commands

Command	Description
show scheduler	Displays the scheduler configuration.

clock protocol

To set the synchronization protocol for the clock to a protocol, use the **clock protocol** command. To remove the clock protocol, use the **no** form of this command.

clock protocol {**none** | **ntp** | **ptp**}

no clock protocol {**none** | **ntp** | **ptp**}

Syntax Description

none	Specifies that the clock can be set manually.
ntp	Specifies that the clock be set to the Network Time Protocol (NTP).
ptp	Specifies that the clock be set to the Precision Time Protocol (PTP).

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set the synchronization protocol for the clock to NTP:

```
switch# configure terminal
switch(config)# clock protocol ntp
switch(config)#
```

This example shows how to set the synchronization protocol for the clock to PTP:

```
switch# configure terminal
switch(config)# clock protocol ptp
switch(config)#
```

Related Commands

Command	Description
feature ptp	Enables PTP on the switch.
show ptp clock	Displays the PTP clock information.
show running-config ptp	Displays the PTP running system configuration information.

commit (Call Home)

To commit Call Home configuration changes and distribute the changes to call Cisco Fabric Services (CFS)-enabled devices, use the **commit** command.

commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to commit CFS Call Home configuration changes:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# commit
switch(config-callhome)#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

commit (session)

To commit the current configuration session, use the **commit** command.

commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Session configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to commit the current session:

```
switch# configure session MySession
switch(config-s)# commit
switch(config-s)#
```

Related Commands

Command	Description
configure session	Creates a configuration session.
show configuration session	Displays the contents of the session.
verify	Verifies a session.

contract-id (Call Home)

To configure the optional contract number for the customer, use the **contract-id** command. To remove a contract number, use the **no** form of this command.

contract-id *contract-number*

no contract-id

Syntax Description

contract-number	Contract number. The contract number can be up to 255 alphanumeric characters in free format.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can configure the customer identification information that Cisco Smart Call Home should use. The service agreement includes the customer identification information, such as the customer ID, contract ID, and site ID.

Examples

This example shows how to configure the contract number for the customer:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# contract-id 12095134-1706
switch(config-callhome)#
```

Related Commands

Command	Description
customer-id	Configures the customer number for the switch.
show callhome	Displays a summary of the Call Home configuration.

customer-id (Call Home)

To configure the optional unique identification number for the customer, use the **customer-id** command. To remove a customer number, use the **no** form of this command.

customer-id *customer-no*

no customer-id

Syntax Description

customer-no	Customer number, as specified in the service agreement. The customer number can be up to 255 alphanumeric characters in free format.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can configure the customer identification information that Cisco Smart Call Home should use. The service agreement includes the customer identification information, such as the customer ID, contract ID, and site ID.

Examples

This example shows how to configure a customer number:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# customer-id AXC-1203
switch(config-callhome)#
```

Related Commands

Command	Description
site-id	Configures the site number for the switch.
show callhome	Displays a summary of the Call Home configuration.

description

To add a description to a user policy, use the **description** command. To remove the policy description, use the **no** form of this command.

description *policy-description*

no description *policy-description*

Syntax Descriptiona		
	policy-description	Policy description. The description can be any case-sensitive, alphanumeric string up to 80 characters enclosed by quotation marks.

Defaults

None

Command Modes

Applet configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add a description to a user policy:

```
switch# configure terminal
switch(config)# event manager applet monitorShutdown
switch(config-applet)# description "Monitors interface shutdown"
```

This example shows how to remove the policy description:

```
switch(config-applet)# no description "Monitors interface shutdown"
switch(config-applet)#
```

Related Commands

Command	Description
description	Configures a descriptive string for the policy.
event	Configures the event statement for the policy.
show event-manager policy state	Correlates multiple events in the policy.
tag	Displays information about the status of the configured policy.

description (SPAN, ERSPAN)

To add a description to an Ethernet Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) session configuration, use the **description** command. To remove the description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	String description of the SPAN session configuration. This string is limited to 80 characters.

Command Default

No description is added.

Command Modes

SPAN session configuration mode
ERSPAN session configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.
6.0(2)A1(1)	ERSPAN support was added.

Usage Guidelines

The **description** command is meant to provide a reminder in the configuration to describe what certain SPAN sessions are used for. The description appears in the output of the **show monitor session** and **show running-config monitor** commands.

Examples

This example shows how to add a description for a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 9 type local
switch(config-monitor)# description A Local SPAN session
switch(config-monitor)#
```

This example shows how to add a description for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 9 type erspan-source
switch(config-erspan-src)# description An ERSPAN session
switch(config-erspan-src)#
```

Related Commands

Command	Description
destination (SPAN session)	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 (SPAN session)	Configures a source SPAN port.

destination ip (ERSPAN)

To configure an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination IP address, use the **destination** command. To remove the destination ERSPAN IP address, use the **no** form of this command.

destination ip *ip_address*

no destination ip *ip_address*

Syntax Description

ip_address	IPv4 address in the format *A.B.C.D*.

Command Default

None

Command Modes

ERSPAN source configuration mode

Command History

Release	Modification
6.0(2A1(1)	This command was introduced.

Usage Guidelines

You can configure only one destination IP address for an ERSPAN source session.

This command does not require a license.

Examples

This example shows how to configure an ERSPAN destination IP address:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# destination ip 192.0.3.1
switch(config-erspan-src)#
```

Related Commands

Command	Description
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 (SPAN session)	Configures a source SPAN port.
source (ERSPAN session)	Configures a source VLAN interface.

destination interface (ERSPAN)

To configure interfaces for an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination, use the **destination interface** command. To remove the interfaces from an ERSPAN session, use the **no** form of this command.

destination interface ethernet *slot*/*port*

no destination interface ethernet *slot*/*port*

Syntax Description

ethernet	Specifies the Ethernet interface.
slot/*port*	Ethernet interface slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.

Command Default

None

Command Modes

ERSPAN destination configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

The destination port should be previously configured as a switchport monitor.

This command does not require a license.

Examples

This example shows how to configure an ERSPAN destination interface:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-destination
switch(config-erspan-dst)# destination interface ethernet 1/5
switch(config-erspan-dst)#
```

Related Commands

Command	Description
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 (SPAN session)	Configures a source SPAN port.
source (ERSPAN session)	Configures a source VLAN interface.

destination-profile (Call Home)

To create a user-defined destination profile, modify a predefined or user-defined destination profile, or configure the message format for that new destination profile, use the **destination-profile** command. To remove the destination profile, use the **no** form of this command.

destination-profile {**CiscoTAC-1** | {{**full-txt-destination** | **short-txt-destination**}{**message-level** *level* | **message-size** *size*}}} {**alert-group** *alert* | **email-addr** *email-address* | **http** *url* | **transport-method** {**email** | **http**}}

destination-profile *profile-name* [**alert-group** *alert* | **email-addr** *email-address* | **format** {**XML** | **full-txt** | **short-txt**} | **http** *url* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}]

no destination-profile

Syntax Description

CiscoTAC-1	Configures a destination profile for Extensible Markup Language (XML) messages.
full-txt-destination	Configures a destination profile for plain text messages.
short-txt-destination	Configures a destination profile for short text message.
message-level *level*	Specifies the Call Home message severity level. The range is from 0 to 9, with 0 being the lowest urgency, and 9 the highest urgency.
message-size *size*	Specifies the maximum message size. The range is as follows: • **full-txt-destination**—From 0 to 5000000, and the default is 2500000. • **short-txt-destination**—From 0 to 100000, and the default is 4000. • **CiscoTAC-1**—5000000, which is not changeable.
alert-group *alert*	Associates one or more alert groups with a destination profile. The *alert* group can be one of the following: • **All**—All alert groups • **Cisco-TAC**—Cisco TAC events • **Configuration**—Configuration events • **Diagnostic**—Diagnostic events • **EEM**—EEM events • **Environmental**—Power, fan, and temperature-related events • **Inventory**—Inventory status events • **License**—Licensing events • **Linecard-Hardware**—Linecard-related events • **Supervisor-Hardware**—Supervisor-related events • **Syslog-group-port**—Syslog message events filed by the port manager • **System**—Software-related events • **Test**—User-generated test events
email-addr	Specifies the e-mail address to which the alert should be sent.

email-address	E-mail address in email address format. The address can be a maximum of 255 alphanumeric characters and cannot contain white spaces; for example, *personname@companyname.com*.
http *url*	Specifies the HTTP or HTTPS URL. The *url* can be a maximum of 255 alphanumeric characters and cannot contain white spaces; for example, http://site.com/services/callserv https://site2.com/serv/CALL
transport-method	Specifies the transport method for sending Call Home messages.
email	Specifies that Call Home messages be sent through e-mail.
http	Specifies that Call Home messages be sent using HTTP.
profile-name	User-defined profile name. The profile name can be a maximum of 31 alphanumeric characters.
format	(Optional) Specifies the Call Home message format. The default is XML.
XML	Specifies that the Call Home message format is XML.
full-txt	Specifies that the Call Home message format is plain text.
short-txt	Specifies that the Call Home message format is a short text message.

Command Default

Message format: XML.

Message size: 2500000 for full-txt-destination, 4000 for short-txt-destination, and 4000000 for XML format.

Message level: 0

Alert group: All for full-text-destination and short-text-destination profiles. The cisco-tac alert group for the CiscoTAC-1 destination profile.

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can modify the following attributes for a predefined or user-defined destination profile:

- Destination e-mail address—The e-mail address to which the alert should be sent.
- Message formatting—The message format used for sending the alert (full text, short text, or XML).
- Message level—The Call Home message severity level for this destination profile.
- Message size—The allowed length of a Call Home message sent to the e-mail addresses in this destination profile.

Note You cannot modify or delete the CiscoTAC-1 destination profile.

The Cisco Nexus 3548 switch does not generate an alert if the Call Home severity level of the alert is lower than the message severity level set for the destination profile.

Table 1-1 lists each Call Home message level keyword.

Table 1-1 Call Home Message Severity Level

Call Home Level	Keyword	Description
9	Catastrophic	Network-wide catastrophic failure.
8	Disaster	Significant network impact.
7	Fatal	System is unusable.
6	Critical	Critical conditions that indicate that immediate attention is needed.
5	Major	Major conditions.
4	Minor	Minor conditions.
3	Warning	Warning conditions.
2	Notification	Basic notification and informational messages.
1	Normal	Normal event signifying return to normal state.
0	Debugging	Debugging messages.

Examples

This example shows how to create a user-defined Call Home destination profile to send Call Home messages through e-mail:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# destination-profile myProfile alert-group Configuration
email-addr myname@somecompany.com message-level 3 transport-method email
switch(config-callhome)#
```

Related Commands

Command	Description
callhome	Configures a Call Home service.
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.
show callhome destination-profile	Displays Call Home information for a destination profile.

diagnostic bootup level

To configure the bootup diagnostic level to trigger diagnostics when the device boots, use the **diagnostic bootup level** command. To remove bootup diagnostic level configuration, use the **no** form of this command.

diagnostic bootup level {**bypass** | **complete**}

no diagnostic bootup level {**bypass** | **complete**}

Syntax Description

bypass	Specifies that all bootup tests are skipped.
complete	Specifies that all bootup diagnostics are performed. This is the default value.

Command Default

Complete

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure the bootup diagnostics level to trigger the complete diagnostics:

```
switch# configure terminal
switch(config)# diagnostic bootup level complete
switch(config)#
```

This example shows how to remove the bootup diagnostics level configuration:

```
switch# configure terminal
switch(config)# no diagnostic bootup level complete
switch(config)#
```

Related Commands

Command	Description
show diagnostic bootup level	Displays the bootup diagnostics level.
show diagnostic bootup result	Displays the results of the diagnostics tests.

distribute (Call Home)

To enable Call Home distribution using Cisco Fabric Services (CFS), use the **distribute** command. To disable Call Home distribution, use the **no** form of this command.

distribute

no distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to enable CFS distribution for Call Home:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# distribute
switch(config-callhome)#
```

This example shows how to disable CFS distribution for Call Home:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# no distribute
switch(config-callhome)#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

duplicate-message throttle (Call Home)

To limit the number of duplicate messages received for the same event, use the **duplicate-message throttle** command. To disable duplicate message throttling for Call Home, use the **no** form of this command.

duplicate-message throttle

no duplicate-message throttle

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

By default, the switch limits the number of duplicate messages received for the same event. If the number of duplicate messages sent exceeds 30 messages within a 2-hour time frame, then the switch discards further messages for that alert type.

Examples

This example shows how to enable duplicate alert message throttling for Call Home:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# duplicate-message throttle
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.

email-contact (Call Home)

To configure the e-mail address for the primary person responsible for the switch, use the **email-contact** command. To remove an email contact, use the **no** form of this command.

email-contact *email-address*

no email-contact

Syntax Description

email-address	E-mail address. The address can be a maximum of 255 alphanumeric characters in e-mail address format and cannot contain spaces.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure an e-mail address:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# email-contact abc@xyz.com
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
phone-contact	Configures the phone number for the primary person responsible for the switch.
show callhome	Displays a summary of the Call Home configuration.

enable (Call Home)

To enable the Cisco Smart Call Home service after you have configured the contact information, use the **enable** command. To disable the Smart Call Home service, use the **no** form of this command.

enable

no enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You must configure an e-mail server. Your switch must have IP connectivity to an e-mail server. You must configure the contact name (SNMP server contact), phone, and street address information before you enable Call Home.

Examples

This example shows how to enable the Cisco Smart Call Home service:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# enable
contact email address is not configured
callhome can not be enabled on the switch, because necessary configuration has not been
done
Please check if all of following configuration is done
contact person name(sysContact)
contact person's email
contact person's phone number
street addr
To configure sysContact, please use snmp-server command
switch(config-callhome)#
```

This example shows how to disable the Cisco Smart Call Home service:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# no enable
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
email-contact	Configures the e-mail address.
show callhome	Displays a summary of the Call Home configuration.

feature ptp

To enable the Precision Time Protocol (PTP) feature, use the **feature ptp** command. To disable the PTP feature, use the **no** form of this command.

feature ptp

no feature ptp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the PTP feature:

```
switch# configure terminal
switch(config)# feature ptp
switch(config)#
```

This example shows how to disable the PTP feature:

```
switch# configure terminal
switch(config)# no feature ptp
switch(config)#
```

Related Commands

Command	Description
ptp source	Configures the source IP address for all PTP packets.
ptp domain	Configures the domain number to use for this clock.
ptp priority1	Configures the priority1 value to use when advertising this clock.
ptp priority2	Configures the priority2 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

feature scheduler

To enable the scheduler feature on a Cisco NX-OS device, use the **feature scheduler** command. To disable the schedule feature, use the **no** form of this command.

feature scheduler

no feature scheduler

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the scheduler feature on a Cisco NX-OS device:

```
switch# configure terminal
switch(config)# feature scheduler
```

This example shows how to disable the scheduler feature on a Cisco NX-OS device:

```
switch(config)# no feature scheduler
switch(config)#
```

Related Commands

Command	Description
scheduler	Configures maintenance jobs.

filter

To filter out specific SPAN or ERSPAN traffic flows that must be monitored, use the **filter** command. To remove the filter, use the **no** form of this command.

filter {**ip** *source-ip-address source-ip-mask destination-ip-address destination-ip-mask* | **mac** *source-mac-address source-mac-mask destination-mac-address destination-mac-mask*}

no filter {**ip** *source-ip-address source-ip-mask destination-ip-address destination-ip-mask* | **mac** *source-mac-address source-mac-mask destination-mac-address destination-mac-mask*}

Syntax Description

ip	Specifies IP-based filtering.
source-ip-address	Specifies the source IP address.
source-ip-mask	Specifies the source IP mask.
destination-ip-address	Specifies the destination IP address.
destination-ip-mask	Specifies the destination IP mask.
mac	Specified MAC-based filtering.
source-mac-address	Specifies the source MAC address.
source-mac-mask	Specifies the source MAC mask.
destination-mac-address	Specifies the destination MAC address.
destination-mac-mask	Specifies the destination MAC mask.

Defaults

Disabled

Command Modes

Monitor configuration mode (SPAN)

ERSPAN source configuration mode (ERSPAN)

Command History

Release	Modification
6.0(2)A4(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to configure an IP-based SPAN filter for a local session:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 1
switch(config-monitor)# source interface Ethernet 1/7 rx
switch(config-monitor)# filter ip 10.1.1.1 255.255.255.0 20.1.1.1 255.255.255.0
switch(config-monitor)# destination interface Ethernet 1/48
switch(config-monitor)# no shut
switch(config-monitor)#
```

The following example shows how to configure a MAC-based SPAN filter for a local session:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 4
switch(config-monitor)# source interface Ethernet 1/6 rx
switch(config-monitor)# filter mac abcd.ef12.3456 1111.2222.3333 1234.5678.9012
111.2222.3333
switch(config-monitor)# destination interface Ethernet 1/48
switch(config-monitor)#
```

The following example shows how to configure an MAC-based filter for an ERSPAN-source session:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 2 type erspan-source
switch(config-erspan-src)# filter mac abcd.ef12.3456 1111.2222.3333 1234.5678.9012
1111.2222.3333
switch(config-erspan-src)# erspan-id 20
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 200.1.1.1
switch(config-erspan-src)# source interface Ethernet 1/47 rx
switch(config-erspan-src)# no shut
switch(config-erspan-src)#
```

The following example shows how to configure a VLAN-based filter for an ERSPAN-source session:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 2 type erspan-source
switch(config-erspan-src)# filter mac abcd.ef12.3456 1111.2222.3333 1234.5678.9012
1111.2222.3333
switch(config-erspan-src)# erspan-id 21
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 200.1.1.1
switch(config-erspan-src)# source interface Ethernet 1/47 rx
switch(config-erspan-src)# source vlan 315
switch(config-erspan-src)# mtu 200
switch(config-erspan-src)# no shut
switch(config-erspan-src)#
```

hardware profile buffer monitor

To enable buffer monitoring, use the **hardware profile buffer monitor** command. To disable buffer monitoring, use the **no** form of this command.

hardware profile buffer monitor {**unicast | multicast**} [**sampling** *interval* | **threshold** *value*]

no hardware profile buffer monitor {**unicast | multicast**} [**sampling** *interval* | **threshold** *value*]

Syntax Descriptionn

unicast	Specifies to enable unicast mode.
multicast	Specifies to enable multicast mode.
sampling	Specifies to monitor the hardware profile buffer by sampling data every second. The default sampling interval is 4 milliseconds.
threshold	Speicifes to generate a syslog entry when the specified maximum buffer threshold is exceeded. The range is from 384 to 6144 kilobytes with 384 kilobyte increments. The default threshold value is 90% of the total available shared buffer.
interval	Sampling interval for hardware. The range is from 10 to 2000000 nanoseconds. The default sampling interval is 4 milliseconds.
value	Histogram threshold value. The range is from ? to ? kilobytes.

Command Modes

Global configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

The following example shows how to configure Active Buffer Monitoring for unicast traffic with a threshold value of 384 kilobytes and a sampling value of 5000 nanoseconds:

```
switch# configure terminal
switch(config)# hardware profile buffer monitor unicast
switch(config)# hardware profile buffer monitor threshold 384
switch(config)# hardware profile buffer monitor unicast sampling 5000
switch(config)# copy running-config startup-config
```

The following example shows how to configure Active Buffer Monitoring for multicast traffic with a threshold value of 384 kilobytes and a sampling value of 5000 nanoseconds.

```
switch# configure terminal
switch(config)# hardware profile buffer monitor multicast
switch(config)# hardware profile buffer monitor threshold 384
switch(config)# hardware profile buffer monitor multicast sampling 5000
```

Related Commandss

Command	Description
show hardware profile buffer monitor	Displays information about whether warp mode is enabled and displays the host, unicast, multicast, and Layer 2 TCAM sizes.

hardware profile forwarding-mode normal

To enable normal mode, use the **hardware profile forwarding-mode normal** command. To disable warp mode, use the **no** form of this command.

hardware profile forwarding-mode normal

hardware profile forwarding-mode normal lpm-entry *ipv4* **multicast-entry** *multicast*

no hardware profile forwarding-mode normal

no hardware profile forwarding-mode normal lpm-entry *ipv4* **multicast-entry** *multicast*

Syntax Description

lpm-entry	Specifies lpm(non-host) entries.
ipv4	The range of values for lpm-entry. Range: 4096-28672.
multicast-entry	Specifies multicast entries.
multicast	The range of values for multicast-entry. Range: 4096-28672.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
6.0(2)A8(1)	This command was introduced.

Usage Guidelines

You must reload the Cisco Nexus 3548 switch after enabling the normal mode and also to revert to the factory default from normal mode.

Examples

This example shows how to enable normal mode:

```
switch(config)# hardware profile forwarding-mode normal
switch(config)#
```

This example shows how to disable normal mode:

```
switch(config)# no hardware profile forwarding-mode normal
```

Related Commands

Command	Description
show hardware profile forwarding-mode	Displays the forwarding-mode status (normal/warp) and the IPv4 and multicast, table size.

hardware profile forwarding-mode warp

To enable warp mode, use the **hardware profile forwarding-mode warp** command. To disable warp mode, use the **no** form of this command.

hardware profile forwarding-mode warp

hardware profile forwarding-mode warp lpm-entry *lpm_warp* **host-entry** *host* **l2-entry** *l2* **multicast-entry** *multicast_warp*

no hardware profile forwarding-mode warp

no hardware profile forwarding-mode warp lpm-entry *lpm_warp* **host-entry** *host* **l2-entry** *l2* **multicast-entry** *multicast_warp*

Syntax Description

lpm-entry	Specifies the lpm (non-host) entries.
ipm_warp	The range of values for lmp-entry. Range: 4096-8192.
host-entry	Specifies the ipv4 values.
host	The range of values for host-entry. Range: 4096-16384.
l2-entry	Specifies the Layer 2 entries.
l2	The range of values for l2-entry. Range: 4096-16384.
multicast-entry	Specifies the multicast entries.
multicast_warp	The range of values for multiast-entry. Range: 4096-16384.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.
6.0(2)A8(1)	The option of changing the TCAM carve value was introduced.

Usage Guidelines

You must reload the Cisco Nexus 3548 switch after enabling the warp mode and also to revert to the factory default from warp mode.

In warp mode, these features are not supported: IP redirect, Egress Routed Access Control Lists (RACLs), Port Access Control Lists (PACLs), and Equal-cost Multipathing (ECMP).

Examples

This example shows how to enable warp mode:

```
switch(config)# hardware profile forwarding-mode warp
switch(config)#
```

This example shows how to disable warp mode:

```
switch(config)# no hardware profile forwarding-mode warp
Warning: This configuration has been modified and will take effect only after sa
ving the configuration (copy r s) and reload!
switch(config)#
```

Related Commands

Command	Description
show hardware profile forwarding-mode	Displays the warp mode status and the host, unicast, multicast, and Layer 2 TCAM sizes.

ip access-list (session)

To create an IPv4 access control list (ACL) within a configuration session, use the **ip access-list** command. To remove an ACL from a configuration session, use the **no** form of this command.

ip access-list *ACL-name*

no ip access-list *ACL-name*

Syntax Description

ACL-name	Name of the IPv4 ACL. The name can be up to 64 alphanumeric characters and cannot contain a space or quotation mark.

Command Default

No IPv4 ACLs are defined by default.

Command Modes

Global session configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to create an IPv4 ACL for a configuration session:

```
switch# configure session MySession1
switch(config-s)# ip access-list myACL
switch(config-s-acl)#
```

Related Commands

Command	Description
configure session	Creates a configuration session.
deny	Configures a deny rule in an IPv4 ACL.
permit	Configures a permit rule in an IPv4 ACL.
show configuration session	Displays the contents of the session.

ip domain-list

To configure the IP domain list, use the **ip domain-list** command. To disable the IP domain list, use the **no** form of the command.

ip domain-list *domain-name* [**use-vrf** *name*]

no ip domain-list *domain-name* [**use-vrf** *name*]

Syntax Description

domain-name	Domain name for the IP domain list. The name can be any case-sensitive, alphanumeric string up to 63 characters.
use-vrf *name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain domain name for the IP domain list. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode
VRF context configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-list** command to configure additional domain names for the device. Use the **vrf context** command to enter the VRF context mode to configure additional domain names for a particular VRF.

Examples

This example shows how to configure the IP domain list for the default VRF:

```
switch# configure terminal
switch(config)# ip domain-list Mysite.com
switch(config)#
```

This example shows how to configure the IP domain list for the management VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-list Mysite.com
switch(config-vrf)#
```

This example shows how to configure the IP domain list for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
```

```
switch(config)# ip name-server 192.0.2.1
switch(config)# ip domain-list Mysite2.com
switch(config)#
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

ip domain-lookup

To enable the Domain Name Server (DNS) lookup feature, use the **ip domain-lookup** command. Use the **no** form of this command to disable this feature.

ip domain-lookup

no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-lookup** command to enable DNS.

Examples

This example shows how to configure the DNS server lookup feature:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1
switch(config)# ip domain-lookup
switch(config)#
```

Related Commands

Command	Description
show hosts	Displays information about the DNS.

ip domain-name

To configure a domain name, use the **ip domain-name** command. To delete a domain name, use the **no** form of the command.

ip domain-name *domain-name* [**use-vrf** *name*]

no ip domain-name *domain-name* [**use-vrf** *name*]

Syntax Description

domain-name	Domain name. The name can be any case-sensitive, alphanumeric string up to 63 characters.
use-vrf *name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode
VRF context configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-name** command to configure the domain name for the device. Use the **vrf context** command to enter the VRF context mode to configure the domain monastery for a particular VRF.

Examples

This example shows how to configure the IP domain name for the default VRF:

```
switch# configure terminal
switch(config)# ip domain-name Mysite.com
switch(config)#
```

This example shows how to configure the IP domain name for the management VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-name Mysite.com
switch(config-vrf)#
```

This example shows how to configure the IP domain name for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)#
```

Related Commands

Command	Description
ip domain-list	Configures the IP domain list.
ip domain-lookup	Enables the Domain Name Server (DNS) lookup feature.
show hosts	Displays information about the IP domain name configuration.

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache, use the **ip host** command. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host *name address1* [*address2... address6*]

no ip host *name address1* [*address2... address6*]

Syntax Description

name	Hostname. The *name* can be any case-sensitive, alphanumeric string up to 80 characters.
address1	IPv4 address in the x.x.x.x format.
address2 ... address6	(Optional) Up to five additional IPv4 addresses in the x.x.x.x format.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use the **ip host** command to add a static host name to DNS.

Examples

This example shows how to configure a static hostname:

```
switch# configure terminal
switch(config)# ip host mycompany.com 192.0.2.1
switch(config)#
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

ip name-server

To configure a name server, use the **ip name-server** command. To disable this feature, use the **no** form of the command.

ip name-server *ip-address* [**use-vrf** *name*]

no ip name-server *ip-address* [**use-vrf** *name*]

Syntax Description

ip-address	IP address for the name server.
use-vrf *name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use to reach the name-server. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode
VRF context configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use the **ip name-server** command to configure the name server for the device. Use the **vrf context** command to enter the VRF context mode to configure the domain names for a particular VRF.

Examples

This example shows how to configure the IP name server for the default VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1
switch(config)#
```

This example shows how to configure the IP name server for the management VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# ip name-server 192.0.2.1
switch(config-vrf)#
```

This example shows how to configure the IP name server for the default VRF to use the management VRF as a backup if the IP name server cannot be reached through the default VRF:

```
switch# configure terminal
switch(config)# vrf context management
switch(config-vrf)# exit
```

```
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1 use-vrf management
switch(config)#
```

Related Commands

Command	Description
ip domain-list	Defines a list of domains.
ip domain lookup	Enables DNS-based host name-to-address translation.
show hosts	Displays information about the IP domain name configuration.
vrf context	Creates a virtual routing and forwarding (VRF) instance.

ip port access-group (session)

To apply an IPv4 access control list (ACL) to an interface as a port ACL, use the **ip port access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

ip port access-group *access-list-name* {**in** | **out**}

no ip port access-group *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Name of the IPv4 ACL. The name can be up to 64 alphanumeric, case-sensitive characters.
in	Specifies that the ACL applies to inbound traffic.
out	Specifies that the ACL applies to outbound traffic.

Command Default

None

Command Modes

Session interface configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to apply an IPv4 ACL named ip-acl-01 to the Ethernet interface 1/2 as a port ACL:

```
switch# configure session MySession1
switch(config-s)# interface ethernet 1/2
switch(config-s-if)# ip port access-group ip-acl-01 in
switch(config-s-if)#
```

This example shows how to remove an IPv4 ACL named ip-acl-01 from Ethernet interface 1/2:

```
switch(config-s)# interface ethernet 1/2
switch(config-s-if)# no ip port access-group ip-acl-01 in
switch(config-s-if)#
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.
show configuration session	Displays the contents of the session.

logging abort

To discard the pending changes to the syslog server configuration, use the **logging abort** command.

logging abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to discard the changes made to the syslog server configuration:

```
switch# configure terminal
switch(config)# logging distribute
switch(config)# logging abort
switch(config)#
```

Related Commands

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the CFS infrastructure.
show logging pending	Displays the pending changes to the syslog server configuration.
show logging status	Displays the logging status.

logging commit

To commit the pending changes to the syslog server configuration for distribution to the switches in the fabric, use the **logging commit** command.

logging commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to commit the distribution of the syslog server configuration:

```
switch# configure terminal
switch(config)# logging distribute
switch(config)# logging commit
switch(config)#
```

Related Commands

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the CFS infrastructure.
show logging status	Displays the logging status.

logging console

To enable logging messages to the console session, use the **logging console** command. To disable logging messages to the console session, use the **no** form of this command.

logging console [*severity-level*]

no logging console

Syntax Description

severity-level	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition—default level • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:

```
switch# configure terminal
switch(config)# logging console 4
switch(config)#
```

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

logging distribute

To enable the distribution of the syslog server configuration to network switches using the Cisco Fabric Services (CFS) infrastructure, use the **logging distribute** command. To disable the distribution, use the **no** form of this command.

logging distribute

no logging distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Distribution is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to enable the distribution of the syslog server configuration:

```
switch# configure terminal
switch(config)# logging distribute
switch(config)#
```

This example shows how to disable the distribution of the syslog server configuration:

```
switch# configure terminal
switch(config)# no logging distribute
switch(config)#
```

Related Commands

Command	Description
logging abort	Cancels the pending changes to the syslog server configuration.
logging commit	Commits the changes to the syslog server configuration for distribution to the switches in the fabric.
show logging status	Displays the logging status.

logging event

To log interface events, use the **logging event** command. To disable logging of interface events, use the **no** form of this command.

logging event {**link-status** | **trunk-status**} {**default** | **enable**}

no logging event {**link-status** | **trunk-status**} {**default** | **enable**}

Syntax Description

link-status	Specifies to log all UP/DOWN and CHANGE messages.
trunk-status	Specifies to log all TRUNK status messages.
default	Specifies to the default logging configuration is used by interfaces not explicitly configured.
enable	Enables the logging to override the port level configuration.

Command Default

None

Command Modes

Global configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.
5.0(3)A1(1)	Support to log interface events was added in switch profiles.

Examples

This example shows how to log interface events:

```
switch# configure terminal
switch(config)# logging event link-status default
switch(config)#
```

This example shows how to log TRUNK interface events in a switch profile:

```
switch# configure 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)# logging event trunk-status default
switch(config-sync-sp)#
```

Related Commands

Command	Description
show logging	Displays the logging status.
show switch-profile	Displays information about the switch profile and the configuration revision.
switch-profile	Creates or configures a switch profile.

logging event port

To log events on an interface, use the **logging event port** command. To disable logging of interface events, use the **no** form of this command.

logging event port {**link-status** | **trunk-status**} [**default**]

no logging event port {**link-status** | **trunk-status**}

Syntax Description

link-status	Specifies to log all UP/DOWN and CHANGE messages.
trunk-status	Specifies to log all TRUNK status messages.
default	(Optional) Specifies the default logging configuration that is used by interfaces not explicitly configured.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to log interface events:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# logging event port link-status default
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.
show logging	Displays the logging status.

logging level

To enable logging messages from a defined facility that have the specified severity level or higher, use the **logging level** command. To disable logging messages from a defined facility, use the **no** form of this command.

logging level *facility severity-level*

no logging level *facility severity-level*

Syntax Description

facility	Facility. To apply the same severity level to all facilities, use the **all** facility.
severity-level	Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition—default level • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to enable logging messages from the AAA facility that have a severity level of 2 or higher:

```
switch# configure terminal
switch(config)# logging level aaa 2
switch(config)#
```

Related Commands

Command	Description
show logging level	Displays the facility logging level configuration.

logging logfile

To configure the name of the log file used to store system messages and the minimum severity level to log, use the **logging logfile** command. To disable logging to the log file, use the **no** form of this command.

logging logfile *logfile-name severity-level* [**size** *bytes*]

no logging logfile [*logfile-name severity-level* [**size** *bytes*]]]

Syntax Description

logfile-name	Name of the log file to be used to store system messages.
severity-level	Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition—default level • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only
size *bytes*	(Optional) Specifies a maximum file size. The default file size is 4194304 bytes and can be configured from 4096 to 4194304 bytes.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure a log file called logfile to store system messages and set its severity level to 4:

```
switch# configure terminal
switch(config)# logging logfile logfile 4
switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the log file.

logging module

To enable module log messages, use the **logging module** command. To disable module log messages, use the **no** form of this command.

logging module [*severity-level*]

no logging module

Syntax Description

severity-level	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows*:* • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition—default level • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Set a specified severity level or use the default.

Examples

This example shows how to enable module log messages:

```
switch# configure terminal
switch(config)# logging module
switch(config)#
```

Related Commands

Command	Description
show logging module	Displays the module logging status.

logging monitor

To enable the device to log messages to the monitor (terminal line), use the **logging monitor** command. To disable monitor log messages, use the **no** form of this command.

logging monitor [*severity-level*]

no logging monitor

Syntax Description

severity-level	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition—default level • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This configuration applies to Telnet and Secure Shell (SSH) sessions.

Examples

This example shows how to enable monitor log messages:

```
switch# configure terminal
switch(config)# logging monitor
switch(config)#
```

Related Commands

Command	Description
show logging monitor	Displays the status of monitor logging.

logging server

To configure a remote syslog server at the specified hostname or IPv4 address, use the **logging server** command. To disable the remote syslog server, use the **no** form of this command.

logging server *host* [*severity-level*] [**facility** *facility* | **use-vrf** {*vrf_name* | **management**}]

no logging server *host* [*severity-level*] [**facility** *facility* | **use-vrf** {*vrf_name* | **management**}]

Syntax Description

host	Hostname or IPv4 address of the remote syslog server.
severity-level	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition—default level • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only
facility *facility*	(Optional) Specifies the outgoing *facility*. The facility can be one of the following: **auth**, **authpriv**, **cron**, **daemon**, **ftp**, **kernel**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**, **lpr**, **mail**, **news**, **syslog**, **user**, **uucp** The default outgoing facility is **local7**.
vrf *vrf_name*	(Optional) Specifies the virtual routing and forwarding (VRF) to be used in the remote server. The name can be a maximum of 32 alphanumeric characters.
management	Specifies the management VRF. This is the default VRF.

Command Default

The default outgoing facility is **local7**.

The default VRF is **management**.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure a remote syslog server at a specified IPv4 address, using the default outgoing facility:

```
switch# configure terminal
switch(config)# logging server 192.168.2.253
switch(config)#
```

This example shows how to configure a remote syslog server at a specified hostname with severity level 5 or higher:

```
switch# configure terminal
switch(config)# logging server syslogA 5
switch(config)#
```

Related Commands

Command	Description
show logging server	Displays the configured syslog servers.

logging timestamp

To set the logging time-stamp units, use the **logging timestamp** command. To reset the logging time-stamp units to the default, use the **no** form of this command.

logging timestamp {**microseconds** | **milliseconds** | **seconds**}

no logging timestamp {**microseconds** | **milliseconds** | **seconds**}

Syntax Description

microseconds	Specifies the units to use for logging timestamps in microseconds. The default units are **seconds**.
milliseconds	Specifies the units to use for logging timestamps in milliseconds.
seconds	Specifies the units to use for logging timestamps in seconds. The default units are **seconds**.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

By default, the units are seconds.

Examples

This example shows how to set the logging time-stamp units to microseconds:

```
switch# configure terminal
switch(config)# logging timestamp microseconds
switch(config)#
```

Related Commands

Command	Description
show logging timestamp	Displays the logging time-stamp configuration.

monitor erspan origin ip-address

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) global origin IP address, use the **monitor espan origin ip-address** command. To remove the ERSPAN global origin IP address configuration, use the **no** form of this command.

monitor erspan origin ip-address *ip-address* [**global**]

no monitor erspan origin ip-address *ip-address* [**global**]

Syntax Description

ip-address	IP address.
global	(Optional) Specifies the default global configuration.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

When you change the origin IP address, it impacts all the sessions.

Note On a Cisco Nexus 3548 Switch switch, only global origin IP address is supported.

This command does not require a license.

Examples

This example shows how to configure the ERSPAN global origin IP address:

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 10.1.1.1 global
switch(config)#
```

This example shows how to remove the ERSPAN global origin IP address:

```
switch# configure terminal
switch(config)# no monitor erspan origin ip-address 10.1.1.1 global
switch(config)#
```

Related Commands

Command	Description
monitor session	Configures a SPAN or an ERSPAN session.

monitor session

To create a new Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) session configuration for analyzing traffic between ports, or add to an existing session configuration, use the **monitor session** command. To clear SPAN sessions, use the **no** form of this command.

monitor session {*session-number* [**shut** | **type** {**local** | **erspan-destination** | **erspan-source**}] | **all shut**}

no monitor session {*session-number* | **all**} [**shut**]

Syntax Description

session-number	SPAN session to create or configure. The range is from 1 to 18.
all	Specifies to apply configuration information to all SPAN sessions.
shut	(Optional) Specifies that the selected session will be shut down for monitoring.
type	(Optional) Specifies the type of session to configure.
local	Specifies the session type to be local.
erspan-destination	Creates an ERSPAN destination session.
erspan-source	Creates an ERSPAN source session.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

To ensure that you are working with a completely new session, you can clear the desired session number or all SPAN sessions.

After you create an ERSPAN session, you can describe the session and add interfaces and VLANs as sources and destinations.

This command does not require a license.

Examples

This example shows how to create a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config)#
```

This example shows how to enter the monitor configuration mode for configuring SPAN session number 9 for analyzing traffic between ports:

```
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)# destination interface ethernet 1/2
switch(config-monitor)# no shutdown
switch(config-monitor)#
```

This example shows how to configure any SPAN destination interfaces as Layer 2 SPAN monitor ports before activating the SPAN session:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to configure a typical SPAN destination trunk interface:

```
switch# configure terminal
switch(config)# interface Ethernet1/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport monitor
switch(config-if)# switchport trunk allowed vlan 10-12
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to create an ERSPAN session:

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

Related Commands

Command	Description
description (SPAN, ERSPAN)	Adds a description to identify the SPAN session.
destination (ERSPAN)	Configures the destination IP port for an ERSPAN packet.
ip dscp (ERSPAN)	Sets the DSCP value for an ERSPAN packet.
ip ttl (ERSPAN)	Sets the time-to-live (TTL) value for an ERSPAN packet.
mtu (ERSPAN)	Sets the maximum transmission value (MTU) for ERSPAN packets.
show monitor session	Displays SPAN session configuration information.
source (SPAN, ERSPAN)	Adds a SPAN source port.

mtu

To configure the truncation of source packets for each SPAN or ERSPAN session based on the size of their MTU, use the **mtu** command. To remove the truncation, use the **no** form of this command.

mtu *size*

no mtu *size*

Syntax Description

size	Configures the MTU size for truncation. Any SPAN packet that is larger than the configured MTU size is truncated to the configured size with a 4-byte offset. The MTU truncation size is between 64 bytes and 1518 bytes.

Defaults

Disabled

Command Modes

Monitor configuration mode (SPAN)

ERSPAN source configuration mode (ERSPAN)

Command History

Release	Modification
6.0(2)A4(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to configure MTU truncation for a local session:

```
switch# configure terminal
switch(config)# monitor session 5
switch(config-monitor)# source interface ethernet 1/5 both
switch(config-monitor)# mtu 512
switch(config-monitor)# destination interface Ethernet 1/39
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 5
session 5
---------------
type : local
state : down (No operational src/dst)
mtu : 512
source intf :
rx : Eth1/5
tx : Eth1/5
both : Eth1/5
source VLANs :
rx :
destination ports : Eth1/39
Legend: f = forwarding enabled, l = learning enabled
```

The following example shows how to configure MTU truncation for an ERSPAN-source session:

```
switch# configure terminal
switch(config)# monitor session 6 type erspan-source
switch(config-erspan-src)# mtu 1096
switch(config-erspan-src)# erspan-id 40
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 200.1.1.1
switch(config-erspan-src)# source interface ethernet 1/40
switch(config-erspan-src)# show monitor session 6
session 6
---------------
type : erspan-source
state : down (Session admin shut)
granularity : 100 microseconds
erspan-id : 40
vrf-name : default
destination-ip : 200.1.1.1
ip-ttl : 255
ip-dscp : 0
header-type : 2
mtu : 1096
origin-ip : 150.1.1.1 (global)
source intf :
rx : Eth1/40
tx : Eth1/40
both : Eth1/40
source VLANs :
rx :
```

ntp

To configure the Network Time Protocol (NTP) peers and servers for the switch, use the **ntp** command. To remove configured peers and servers, use the **no** form of this command.

ntp {**peer** *hostname* | **server** *hostname*} [**prefer**] [**use-vrf** *vrf-name*]

no ntp {**peer** *hostname* | **server** *hostname*}

Syntax Description

peer *hostname*	Specifies the hostname or IP address of an NTP peer.
server *hostname*	Specifies the hostname or IP address of the NTP server.
prefer	(Optional) Specifies this peer/server as the preferred peer/server.
use-vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) used to reach this peer/server.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can specify multiple peer associations.

Examples

This example shows how to form a server association with a server:

```
switch# configure terminal
switch(config)# ntp server ntp.cisco.com
switch(config)#
```

This example shows how to form a peer association with a peer:

```
switch# configure terminal
switch(config)# ntp peer 192.168.10.0
switch(config)#
```

This example shows how to delete an association with a peer:

```
switch# configure terminal
switch(config)# no ntp peer 192.168.10.0
switch(config)#
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

ntp abort

To discard the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress, use the **ntp abort** command.

ntp abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to discard the NTP CFS distribution session in progress:

```
switch# configure terminal
switch(config)# ntp abort
switch(config)#
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

ntp authenticate

To prevent the system from synchronizing with unauthenticated, unconfigured network peers, use the **ntp authenticate** command. Use the **no** form of this commend to allow synchronization with unauthenticated, unconfirmed network peers.

ntp authenticate

no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

If the system has been configured with the **ntp passive**, **ntp broadcast client**, or **ntp multicast client** commands, when NTP receives an incoming symmetric active, broadcast, or multicast packet, it can set up an ephemeral peer association in order to synchronize with the sender.

If **ntp authenticate** is specified, when a symmetric active, broadcast, or multicast packet is received, the system will not synchronize to the peer unless the packet carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

To prevent synchronization with unauthorized network hosts, **ntp authenticate** should be specified any time **ntp passive**, **ntp broadcast client**, or **ntp multicast client** has been specified unless other measures, such as the **ntp access-group** command, have been taken to prevent unauthorized hosts from communicating with the NTP service on the device.

Note This command does not authenticate peer associations configured via the **ntp server** and **ntp peer** commands. To authenticate ntp server and ntp peer associations, specify the **key** keyword.

Related Commands

Command	Description
ntp authentication-key	Configures an NTP authentication key.
ntp trusted-key	Specifies one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it.
show ntp authentication-status	Displays the status of NTP authentication.

ntp commit

To apply the pending configuration pertaining to the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ntp commit** command.

ntp commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to commit changes to the active NTP configuration:

```
switch# configure terminal
switch(config)# ntp commit
switch(config)#
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

ntp distribute

To enable Cisco Fabric Services (CFS) distribution for Network Time Protocol (NTP), use the **ntp distribute** command. To disable this feature, use the **no** form of this command.

ntp distribute

no ntp distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **ntp commit** command.

Examples

This example shows how to distribute the active NTP configuration to the fabric:

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)#
```

Related Commands

Command	Description
ntp commit	Commits the NTP configuration changes to the active configuration.
show ntp	Displays NTP information.

ntp sync-retry

To retry synchronization with the configured Network Time Protocol (NTP) servers, use the **ntp sync-retry** command.

ntp sync-retry

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to retry synchronization with the configured NTP servers:

```
switch# ntp sync-retry
switch#
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

periodic-inventory (Call Home)

To configure the switch to periodically send a message with an inventory of all software services currently enabled and running on the device with hardware inventory information, use the **periodic-inventory** command. To disable the periodic messages, use the **no** form of this command.

periodic-inventory notification [**interval** *time-period* | **timeofday** *time-of-day*]

no periodic-inventory notification [**interval** *time-period* | **timeofday** *time-of-day*]

Syntax Description

notification	Enables sending periodic software inventory messages.
interval *time-period*	(Optional) Specifies the time period for periodic inventory notification. The time period range is from 1 to 30 days, and the default is 7 days.
timeofday *time-of-day*	(Optional) Specifies the time of day for periodic inventory notification. The time of day is in HH:MM format.

Command Default

Interval: 7 days

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

The switch generates two Call Home notifications: periodic configuration messages and periodic inventory messages.

Examples

This example shows how to configure a periodic inventory notification to generate every 5 days:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 5
switch(config-callhome)#
```

This example shows how to disable a periodic inventory notification for Call Home:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# no periodic-inventory notification interval 5
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

phone-contact (Call Home)

To configure the phone number for the primary person responsible for the device, use the **phone-contact** command. To remove a phone contact, use the **no** form of this command.

phone-contact *phone-no*

no phone-contact

Syntax Description

phone-no	Phone number in international phone number format, such as +1-800-123-4567. The phone number can be a maximum of 17 alphanumeric characters and cannot contain spaces. **Note** You must use the + prefix before the number.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure a phone number for the primary person responsible for the device:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays a summary of the Call Home configuration.
streetaddress	Configures the street address for the primary person responsible for the switch.

ptp

To enable the Precision Time Protocol (PTP) on an interface, use the **ptp** command. To disable PTP on an interface, use the **no** form of this command.

ptp

no ptp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable PTP on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ptp
switch(config-if)#
```

This example shows how to disable PTP on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp
switch(config-if)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp delay-request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
ptp source	Configures the source IP address for all PTP packets.
ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the PTP VLAN value on an interface.

ptp announce

To configure the interval between Precision Time Protocol (PTP) announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the **ptp announce** command. To remove the interval configuration for PTP messages, use the **no** form of this command.

ptp announce {**interval** *seconds* | **timeout** *count*}

no ptp announce {**interval** *seconds* | **timeout** *count*}

Syntax Description

interval	Specifies the interval between Precision Time Protocol (PTP) announce messages on an interface.
seconds	Log seconds. The range is from 0 to 4.
timeout	Specifies the number of PTP intervals before a timeout occurs on an interface.
count	Timeout count. The range is from 2 to 10.

Command Default

interval 1
timeout 3

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

This command does not require a license.

Examples

This example shows how to configure the interval between PTP announce messages on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ptp announce interval 1
switch(config-if)#
```

This example shows how to remove the interval configuration for PTP messages from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp announce interval 1
switch(config-if)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp	Enables or disables PTP on an interface.
ptp delay-request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
ptp source	Configures the source IP address for all PTP packets.
ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the PTP VLAN value on an interface.

ptp delay-request minimum interval

To configure the minimum interval allowed between Precision Time Protocol (PTP) delay-request messages when the port is in the master state, use the **ptp delay-request minimum interval** command. To remove the minimum interval configuration for PTP delay-request messages, use the **no** form of this command.

ptp delay-request minimum interval *seconds*

no ptp delay-request minimum interval *seconds*

Syntax Description

seconds	Log seconds. The range is from -1 to 6.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

This command does not require a license.

Examples

This example shows how to configure the minimum interval allowed between PTP delay-request messages:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ptp delay-request minimum interval 3
switch(config-if)#
```

This example shows how to remove the minimum interval configuration for PTP delay-request messages:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp delay-request minimum interval 3
switch(config-if)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp	Enables or disables PTP on an interface.

Command	Description
ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
ptp source	Configures the source IP address for all PTP packets.
ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the PTP VLAN value on an interface.

ptp domain

To configure a domain number for the Precision Time Protocol (PTP) clock, use the **ptp domain** command. To remove the domain configuration for the PTP clock, use the **no** form of this command.

ptp domain *domain_number*

no ptp domain *domain_number*

Syntax Description

domain_number	Domain number. The range is from 0 to 128.

Command Default

0

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a domain number for the PTP clock:

```
switch# configure terminal
switch(config)# ptp domain 6
switch(config)#
```

This example shows how to remove the PTP domain configuration:

```
switch# configure terminal
switch(config)# no ptp domain 6
switch(config)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp priority1	Configures the priority1 value to use when advertising this clock.
ptp priority2	Configures the priority2 value to use when advertising this clock.
ptp source	Configures the source IP address for all PTP packets.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

ptp priority1

To configure the priority1 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority1** command. To remove the priority1 value, use the **no** form of this command.

ptp priority1 *priority-number*

no ptp priority1 *priority-number*

Syntax Description

priority-number	Priority number. The range is from 0 to 255.

Command Default

255

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the priority1 value when advertising the PTP clock:

```
switch# configure terminal
switch(config)# ptp priority1 10
switch(config)#
```

This example shows how to remove the priority1 value when advertising the PTP clock:

```
switch# configure terminal
switch(config)# no ptp priority1 10
switch(config)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the switch.
ptp source	Configures the source IP address for all PTP packets.
ptp domain	Configures the domain number to use for this clock.
ptp priority2	Configures the priority2 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

ptp priority2

To configure the priority2 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority2** command. To remove the priority2 value when advertising the PTP, use the **no** form of this command.

ptp priority2 *priority-number*

no ptp priority2 *priority-number*

Syntax Description

priority-number	Priority number. The range is from 0 to 255.

Command Default

255

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the priority2 value when advertising the PTP clock:

```
switch# configure terminal
switch(config)# ptp priority2 1
switch(config)#
```

This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:

```
switch# configure terminal
switch(config)# no ptp priority2 1
switch(config)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp source	Configures the source IP address for all PTP packets.
ptp domain	Configures the domain number to use for this clock.
ptp priority1	Configures the priority1 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

ptp source

To configure the global source for all the Precision Time Protocol (PTP) packets, use the **ptp source** command. To remove the global source for PTP packets, use the **no** form of this command.

ptp source *ip_address* [**vrf** {*vrf-name* | **management**]

no ptp source *ip_address* [**vrf** {*vrf-name* | **management**]

Syntax Description

ip_address	IPv4 address of the source.
vrf	Specifies the virtual routing and forwarding (VRF) instance.
vrf-name	Name of the VRF. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
management	Specifies the management VRF.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the global source for all the PTP packets:

```
switch# configure terminal
switch(config)# ptp source 192.0.1.1
switch(config)#
```

This example shows how to remove the global source configuration for all the PTP packets:

```
switch# configure terminal
switch(config)# no ptp source 192.0.1.1
switch(config)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp domain	Configures the domain number to use for this clock.
ptp priority1	Configures the priority1 value to use when advertising this clock.
ptp priority2	Configures the priority2 value to use when advertising this clock.

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

ptp sync interval

To configure the interval between Precision Time Protocol (PTP) synchronization messages on an interface, use the **ptp sync interval** command. To remove the interval configuration for PTP messages synchronization, use the **no** form of this command.

ptp sync interval *seconds*

no ptp sync interval *seconds*

Syntax Description

seconds	Log seconds. The range is from –6 to 1.

Command Default

0

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

A Cisco Nexus 3548 Switch switch must be synchronized on the Slave port with a sync log interval value of less than or equal to -3. Any Master ports on the switch that are connected to downlink Cisco Nexus 3548 Switch switches must be configured for a sync log interval value that is less than or equal to -3.

This command does not require a license.

Examples

This example shows how to configure the interval between PTP synchronization messages on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ptp sync interval 1
switch(config-if)#
```

This example shows how to remove the interval configuration for PTP messages synchronization:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp sync interval 1
switch(config-if)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the switch.
ptp	Enables or disables PTP on an interface.
ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
ptp delay-request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
ptp vlan	Configures the PTP VLAN value on an interface.

ptp vlan

To configure a VLAN to generate the Precision Time Protocol (PTP) messages for Layer 2 interfaces, use the **ptp vlan** command. To remove the PTP VLAN configuration from an interface, use the **no** form of this command.

ptp vlan *vlan-number*

no ptp vlan *vlan-number*

Syntax Description

vlan-number	VLAN number. The range is from 1 to 4094.

Command Default

1

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

Use this command only on Layer 2 Ethernet interfaces (1 Gigabit, 10-Gigabit, 40-Gigabit) or port-channel members.

By default, VLAN 1 is used to generate the PTP messages on an interface. You must explicitly configure the following VLANs to generate PTP messages on interfaces:

- nondefault access VLANs on an access port
- nondefault native VLANs on a trunk port

This command does not require a license.

Examples

This example shows how to configure the PTP VLAN value on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ptp vlan 9
switch(config-if)#
```

This example shows how to remove the PTP VLAN value from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no vlan 9
switch(config-if)#
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the switch.
ptp	Enables or disables PTP on an interface.
ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
ptp delay-request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
ptp sync interval	Configures the interval between PTP synchronization messages on an interface.

rmon alarm

To configure Remote Monitoring (RMON) alarms on any integer-based Simple Network Management Protocol (SNMP) management information base (MIB) object, use the **rmon alarm** command. To remove an RMON alarm, use the **no** form of this command.

rmon alarm *alarm-no MIB-obj sample-interval* {**absolute** | **delta**} **rising-threshold** *rising-threshold-value* {*event-index* **falling-threshold** *fall-threshold-value* [*event-index*] [**owner** *name*] | **falling-threshold** *fall-threshold-value* [*event-index*] [**owner** *name*]}

no rmon alarm *alarm-no MIB-obj sample-interval* {**absolute** | **delta**} **rising-threshold** *rising-threshold-value* {*event-index* **falling-threshold** *fall-threshold-value* [*event-index*] [**owner** *name*] | **falling-threshold** *fall-threshold-value* [*event-index*] [**owner** *name*]}

Syntax Description

alarm-no	Alarm number. The range is from 1 to 65535.
MIB-obj	MIB object to monitor. The MIB object must be an existing SNMP MIB object in standard dot notation; for example, 1.3.6.1.2.1.2.2.1.17.83886080.
sample-interval	Sample interval at which the switch collects a sample value of the MIB object. The range is from 1 to 700000 seconds.
absolute	Specifies the sample type as absolute.
delta	Specifies the sample type as delta.
rising-threshold	Configures the rising threshold value at which the switch triggers a rising alarm or resets a falling alarm.
rising-threshold-value	Rising threshold value. The range is from –2147483648 to 2147483647.
event-index	Event or action that the switch takes when an alarm, rising or falling, triggers. The *event index* range is from 0 to 65535.
falling-threshold	Configures the falling threshold value at which the switch triggers a falling alarm or resets a rising alarm.
fall-threshold-value	Falling threshold value. The range is from –2147483648 to 2147483647. **Note** The falling threshold value must be less than the rising threshold.
owner *name*	(Optional) Specifies an owner for the alarm. The name can be any alphanumeric string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must have configured an SNMP user and enabled SNMP notifications using the **snmp-server user** and **snmp-server enable traps** command, respectively.

You can only configure an RMON alarm on an integer-based SNMP MIB object. The MIB object must be in standard dot notation. For example, 1.3.6.1.2.1.2.2.1.17 represents ifOutOctets.17.

Absolute samples take the current snapshot of the MIB object value. Delta samples take two consecutive samples and calculate the difference between them. For example, you can set a delta type rising alarm on an error counter MIB object. If the error counter delta exceeds this value, you can trigger an event that sends an SNMP notification and logs the rising alarm event. This rising alarm will not occur again until the delta sample for the error counter drops below the falling threshold.

You can associate a particular event to each RMON alarm. RMON supports the following event types:

- SNMP notification—Sends an SNMP risingAlarm or fallingAlarm notification when the associated alarm triggers.
- Log—Adds an entry in the RMON log table when the associated alarm triggers.
- Both—Sends an SNMP notification and adds an entry in the RMON log table when the associated alarm triggers.

You can specify a different event for a falling alarm and a rising alarm.

Examples

This example shows how to configure an RMON alarm:

```
switch(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.17.83886080 5 delta rising-threshold 5 1
falling-threshold 0 owner test
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
snmp-server enable traps	Enables SNMP notifications on the switch.
snmp-server user	Configures an SNMP user.
show rmon	Displays information about RMON alarms and events.

rmon event

To configure Remote Monitoring (RMON) events to associate with RMON alarms, use the **rmon event** command. To remove an RMON event, use the **no** form of this command.

rmon event *event-index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]

no rmon event *event-index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]

Syntax Description

event-index	Event or action that the switch takes when an alarm, rising or falling, triggers. The *event index* range is from 0 to 65535.
description *string*	(Optional) Specifies a description for the event. The description can be any alphanumeric string.
log	(Optional) Specifies that an RMON log be generated when the event occurs.
trap	(Optional) Specifies that an SNMP trap be generated when the event occurs.
owner *name*	(Optional) Specifies an owner for the alarm. The name can be any alphanumeric string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must have configured an SNMP user and enabled SNMP notifications using the **snmp-server user** and **snmp-server enable traps** command, respectively.

You can reuse the same event with multiple RMON alarms.

Examples

This example shows how to configure an RMON event:

```
switch# configure terminal
switch(config)# rmon event 1 owner test
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
snmp-server enable traps	Enables SNMP notifications on the switch.

Command	Description
snmp-server user	Configures an SNMP user.
show rmon	Displays information about RMON alarms and events.

rmon hcalarm

To configure a high-capacity Remote Monitoring (RMON) alarm, use the **rmon hcalarm** command. To remove a high-capacity RMON alarm, use the **no** form of this command.

rmon hcalarm *alarm-no MIB-obj sample-interval* {**absolute** | **delta**} **startupalarm** *startup-alarm-type* **rising-threshold** *rising-threshold-value event-index* **falling-threshold** *fall-threshold-value* [*event-index*] [**owner** *name*]

no rmon hcalarm *alarm-no MIB-obj sample-interval* {**absolute** | **delta**} **startupalarm** *startup-alarm-type* **rising-threshold** *rising-threshold-value event-index* **falling-threshold** *fall-threshold-value* [*event-index*] [**owner** *name*]

Syntax Description

alarm-no	Alarm number. The range is from 1 to 65535.
MIB-obj	MIB object to monitor. The MIB object must be an existing SNMP MIB object in standard dot notation; for example, 1.3.6.1.2.1.2.2.1.17.83886080.
sample-interval	Sample interval at which the switch collects a sample value of the MIB object. The range is from 1 to 700000 seconds.
absolute	Specifies the sample type as absolute.
delta	Specifies the sample type as delta.
startupalarm	Configures the startup alarm type.
startup-alarm-type	Startup alarm type. The range is from 1 to 3, where 1 is rising, 2 is falling, and 3 is rising or falling.
rising-threshold	Configures the rising threshold value at which the switch triggers a rising alarm or resets a falling alarm.
rising-threshold-value	Rising threshold value. The range is from 0 to 18446744073709551615.
event-index	Event or action that the switch takes when an alarm, rising or falling, triggers. The *event index* range is from 0 to 65535.
falling-threshold	Configures the falling threshold value at which the switch triggers a falling alarm or resets a rising alarm.
fall-threshold-value	Falling threshold value. The range is from 0 to 18446744073709551615. **Note** The falling threshold value must be less than the rising threshold.
owner *name*	(Optional) Specifies an owner for the alarm. The name can be any alphanumeric string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must have configured an SNMP user and enabled SNMP notifications using the **snmp-server user** and **snmp-server enable traps** command, respectively.

You can configure a high-capacity RMON alarm on any integer-based SNMP MIB object. The MIB object must be in standard dot notation. For example, 1.3.6.1.2.1.2.2.1.17 represents ifOutOctets.17.

Absolute samples take the current snapshot of the MIB object value. Delta samples take two consecutive samples and calculate the difference between them. For example, you can set a delta type rising alarm on an error counter MIB object. If the error counter delta exceeds this value, you can trigger an event that sends an SNMP notification and logs the rising alarm event. This rising alarm does not occur again until the delta sample for the error counter drops below the falling threshold.

You can associate a particular event to each high-capacity RMON alarm. RMON supports the following event types:

- SNMP notification—Sends an SNMP risingAlarm or fallingAlarm notification when the associated high-capacity alarm triggers.
- Log—Adds an entry in the RMON log table when the associated high-capacity alarm triggers.
- Both—Sends an SNMP notification and adds an entry in the RMON log table when the associated high-capacity alarm triggers.

You can specify a different event for a falling high-capacity alarm and a rising high-capacity alarm.

Examples

This example shows how to configure an RMON high-capacity alarm:

```
switch# configure terminal
switch(config)# rmon hcalarm 3 1.3.6.1.2.1.2.2.1.17.83886080 5 delta startupalarm 3
rising-threshold 5 1 falling-threshold 3 3 owner test
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
snmp-server enable traps	Enables SNMP notifications on the switch.
snmp-server user	Configures an SNMP user.
show rmon	Displays information about RMON alarms and events.

sampling

To configure only a specific sample of source packets that must be monitored, use the **sampling** command. To remove the sampling, use the **no** form of this command.

sample *sampling-range*

no sample *sampling-range*

Syntax Description

sampling-range	Specifies a range for spanning packets. If the range is defined as n, every nth packet will be spanned. The sampling range is between 2 and 1023.

Defaults

Disabled

Command Modes

Monitor configuration mode (SPAN)

ERSPAN source configuration mode (ERSPAN)

Command History

Release	Modification
6.0(2)A4(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to configure sampling on a VLAN for a local session:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 1
switch(config-monitor)# source vlan 100
switch(config-monitor)# sampling 10
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
session 1
---------------
type : local
state : up
sampling : 10
source intf :
rx : Eth1/3 Eth1/7
tx :
both :
source VLANs :
rx : 100
destination ports : Eth1/48
Legend: f = forwarding enabled, l = learning enabled
```

The following example shows how to configure sampling for an ERSPAN-source session:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 2 type erspan-source
switch(config-erspan-src)# sampling 40
switch(config-erspan-src)# erspan-id 30
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 200.1.1.1
switch(config-erspan-src)# source interface ethernet 1/47
switch(config-erspan-src)# show monitor session 2
session 2
---------------
type : erspan-source
state : up
granularity : 100 microseconds
erspan-id : 30
vrf-name : default
destination-ip : 200.1.1.1
ip-ttl : 255
ip-dscp : 0
header-type : 2
mtu : 200
sampling : 40
origin-ip : 150.1.1.1 (global)
source intf :
rx : Eth1/47
tx : Eth1/47
both : Eth1/47
source VLANs :
rx : 315
switch(config-erspan-src)#
```

scheduler

To create or schedule a scheduler job, use the **scheduler** command. To remove a job or scheduled job, use the **no** form of this command.

scheduler {**aaa-authentication** [**username** *username*] **password** [**0** | **7**] *password* |
job name *job-name* | **logfile size** *filesize* | **schedule name** *schedule-name* | **transport email**
[**from** *email address*] [**reply to** *email address*] [**smtp-server**]}

no scheduler {**aaa-authentication** [**username** *username*] **password** [**0** | **7**] *password* |
job name *job-name* | **logfile size** *filesize* | **schedule name** *schedule-name* | **transport email**
[**from** *email address*] [**reply to** *email address*] [**smtp-server**]}

Syntax Description

aaa-authentication	Begins an AAA authentication exchange with a remote user.
username *username*	Indicates the remote user is entering a username and specifies the username. A username can be any case-sensitive, alphanumeric string up to 32 characters.
password	Indicates the remote user is entering a password for authentication.
0	Indicates the password is in clear text.
7	Indicates the password is encrypted.
password	Remote user's password. A password can be any case-sensitive, alphanumeric string up to 64 characters.
job name *job-name*	Places you into job configuration mode for the specified job name. The job name can be any alphanumeric string up to 31 characters.
logfile	Specifies a logfile configuration.
size *filesize*	Specifies the size of the logfile. The range is from 16 to 1024 KB.
schedule	Defines a schedule for a job.
name *schedule-name*	Specifies the name of the schedule. The schedule name can be any alphanumeric string up to 31 characters.
transport	Specifies transport-related configuration.
email	Specifies the e-mail address.
from *email address*	Configures the from e-mail address. An e-mail address can be up to 255 characters in this format: abc@xyz.com.
reply-to *email address*	Configures the reply to e-mail address. An e-mail address can be up to 255 character in this format: abc@xyz.com.
smtp-server	Specifies the Simple Mail Transport Protocol server, which can be a DNS name or an IPv4 address.

Defaults

None

Command Modes

Job configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

To use the **scheduler** command, you must enable the scheduler. To enable the scheduler, use the **feature scheduler** command.

Remote users must authenticate with the device by using the **scheduler aaa-authentication** command before using the **scheduler** command to configure a maintenance job.

Note The commands within a scheduler job must be entered in a single line separated by a semicolon (;).

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create a scheduler job that saves the running configuration to a file in bootflash and then copies the file from bootflash to a TFTP server. The filename is created using the current timestamp and switch name.

```
switch(config)# scheduler job name backup-cfg
switch(config-job)# cli var name timestamp $(TIMESTAMP);copy running-config
bootflash:/$(SWITCHNAME)-cfg.$(timestamp);copy bootflash:/$(SWITCHNAME)-cfg.$(timestamp)
tftp://1.2.3.4/ vrf management
switch(config-job)# end
switch(config)#
```

This example shows how to remove a scheduler job:

```
switch(config)# no scheduler job name backup-cfg
```

This example shows how to schedule a scheduler job to run daily at 12:00 a.m.:

```
switch(config)# scheduler schedule name daily
switch(config-schedule)# job name backup-cfg
switch(config-schedule)# time daily 1:00
switch(config-schedule)# end
switch(config)#
```

This example shows how to remove a scheduler job schedule:

```
switch(config)# no scheduler schedule name daily
```

Related Commands

Command	Description
feature scheduler	Enables the scheduler.
show scheduler	Displays scheduler information.

show callhome

To display the Call Home configuration information, use the **show callhome** command.

show callhome [**pending** | **pending-diff** | **session** | **status**]

Syntax Description

pending	(Optional) Displays the Call Home configuration changes in the pending Cisco Fabric Services (CFS) database.
pending-diff	(Optional) Displays the differences between the pending and running Call Home configuration.
session	(Optional) Displays the status of the last Call Home CFS command.
status	(Optional) Displays the Call Home status.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the Call Home configuration information:

```
switch# show callhome
callhome disabled
Callhome Information:
contact person name(sysContact):who@where
contact person's email:
contact person's phone number:
street addr:
site id:
customer id:
contract id:ac12
switch priority:7
duplicate message throttling : enabled
periodic inventory : enabled
periodic inventory time-period : 7 days
periodic inventory timeofday : 08:00 (HH:MM)
Distribution : Disabled
switch#
```

Related Commands

Command	Description
callhome	Configures a Call Home service.
show callhome destination-profile	Displays Call Home information for a destination profile.

show callhome destination-profile

To display the Call Home destination profile information, use the **show callhome destination-profile** command.

show callhome destination-profile [**profile** {**CiscoTAC-1** | *profile-name* | **full-txt-destination** | **short-txt-destination**}]

Syntax Description

profile	(Optional) Displays information about a specific destination profile.
CiscoTAC-1	(Optional) Displays information for a CiscoTAC-1 destination profile.
profile *profile-name*	(Optional) Displays information for a user-defined destination profile. The name can be a maximum of 32 alphanumeric characters.
full-txt-destination	(Optional) Displays information of a destination profile configured for plain text messages.
short-txt-destination	(Optional) Displays information of a destination profile configured for short text messages.

Command Default

All destination profiles

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display information about the Call Home destination profiles:

```
switch# show callhome destination-profile

full_txt destination profile information
maximum message size:2500000
message format:full-txt
message-level:0
transport-method:email
email addresses configured:

url addresses configured:

alert groups configured:
all

short_txt destination profile information
maximum message size:4000
message format:short-txt
message-level:0
transport-method:email
<--Output truncated-->
switch#
```

This example shows how to display information about a specific Call Home destination profile:

```
switch# show callhome destination-profile profile CiscoTAC-1
CiscoTAC-1 destination profile information
maximum message size:5000000
message-level:0
transport-method:email
email addresses configured:

url addresses configured:

alert groups configured:
cisco-tac


switch#
```

Related Commands

Command	Description
destination-profile	Creates a user-defined Call Home destination profile.
show callhome	Displays a summary of the Call Home configuration.

show callhome transport-email

To display information about the e-mail configuration for Call Home, use the **show callhome transport-email** command.

show callhome transport-email

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the transport configuration for Call Home:

```
switch# show callhome transport-email
from email addr:DCBU-5020-02@cisco.com
reply to email addr:junk@kunk.com
smtp server:192.168.1.236
smtp server port:25
switch#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

show callhome user-def-cmds

To display the user-defined CLI **show** commands added to a Call Home alert group, use the **show callhome user-def-cmds** command.

show callhome user-def-cmds

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the user-defined CLI **show** commands added to an alert group:

```
switch# show callhome user-def-cmds
User configured commands for alert groups :
alert-group configuration user-def-cmd show running-config

switch#
```

Related Commands

Command	Description
alert-group	Adds CLI **show** commands to a Call Home alert group.

show diagnostic bootup level

To display the current bootup diagnostic level on the switch, use the **show diagnostic bootup level** command.

show diagnostic bootup level

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the current bootup diagnostic level:

```
switch# show diagnostic bootup level
```

Related Commands

Command	Description
diagnostic bootup level	Configures the bootup diagnostic level for a faster module bootup time.
show diagnostic result	Displays the results of the diagnostics tests.

show diagnostic result

To display the results of the diagnostic tests, use the **show diagnostic result** command.

show diagnostic result module {*module-no* | **all**}

Syntax Description

module	Specifies the module for which diagnostic results are displayed.
module-no	Module number. Valid values are 1 to 3.
all	Displays the diagnostic results for all modules.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the diagnostic results for a specific module:

```
switch# show diagnostic result module 1
```

Related Commands

Command	Description
diagnostic bootup level	Configures the bootup diagnostic level for a faster module bootup time.
show diagnostic bootup level	Displays the bootup diagnostics level.

show hardware profile buffer monitor summary

To display buffer histogram data, use the **show hardware profile buffer monitor** command.

show hardware profile buffer monitor [buffer-block *block-number* **| multicast** *block-number* **| interface ethernet** *slot/port***] {brief | detail | summary}**

Syntax Description

buffer-block	Specifies to display information about a specific buffer block.
block-number	Number of the buffer block.
multicast	Specifies to display multicast utilization per memory block.
interface ethernet	Specifies to display information about an Ethernet interface.
slot/port	Slot and port number of the interface.
brief	Specifies to show the maximum buffer utilization per buffer block, unicast utilization for a specific interface, or multicast utilization per memory block.
detail	Specifies to display all information gathered for each interface.
summary	Specifies to display maximum buffer utilization per buffer block.

Command Default

Displays hardware profile buffer information for the entire device.

Command Modes

Global or Exec configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

The following example shows how to display summary information for each buffer block and for all of the buffers combined:

```
switch# show hardware profile buffer monitor summary
```

show hardware profile buffer monitor

To display buffer histogram data, use the **show hardware profile buffer monitor** command.

show hardware profile buffer monitor [buffer-block *block-number* **| multicast** *block-number* **| interface ethernet** *slot/port***] {brief | detail | summary}**

Syntax Description

buffer-block	Specifies to display information about a specific buffer block.
block-number	Number of the buffer block.
multicast	Specifies to display multicast utilization per memory block.
interface ethernet	Specifies to display information about an Ethernet interface.
slot/port	Slot and port number of the interface.
brief	Specifies to show the maximum buffer utilization per buffer block, unicast utilization for a specific interface, or multicast utilization per memory block.
detail	Speicifes to display all information gathered for each interface.
summary	Specifies to display maximum buffer utlization per buffer block.

Command Default

Displays hardware profile buffer information for the entire device.

Command Modes

Global or Exec configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

The following example shows how to display summary information for each buffer block and for all of the buffers combined:

```
switch# show hardware profile buffer monitor summary
Summary CLI issued at: 09/18/2012 07:38:39

                    Maximum buffer utilization detected
                  1sec     5sec    60sec     5min      1hr
                 ------   ------   ------   ------   ------
Buffer Block 1       0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Available = 5049 Kbytes
Class Threshold Limit = 4845 Kbytes
============================================================
Buffer Block 2       0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
============================================================
Buffer Block 3       0KB      0KB   5376KB   5376KB      N/A
```

```
Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
```

The following example shows how to display the maximum buffer utilization of each buffer block and each interface for unicast mode:

```
switch# show hardware profile buffer monitor brief
Brief CLI issued at: 09/18/2012 07:38:29

                   Maximum buffer utilization detected
                  1sec     5sec    60sec     5min      1hr
                 ------   ------   ------   ------   ------
Buffer Block 1       0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Avaliable = 5049 Kbytes
Class Threshold Limit = 4845 Kbytes
------------------------------------------------------------
Ethernet1/45         0KB      0KB      0KB      0KB      N/A
Ethernet1/46         0KB      0KB      0KB      0KB      N/A
Ethernet1/47         0KB      0KB      0KB      0KB      N/A
Ethernet1/48         0KB      0KB      0KB      0KB      N/A
Ethernet1/21         0KB      0KB      0KB      0KB      N/A
Ethernet1/22         0KB      0KB      0KB      0KB      N/A
Ethernet1/23         0KB      0KB      0KB      0KB      N/A
Ethernet1/24         0KB      0KB      0KB      0KB      N/A
Ethernet1/9          0KB      0KB      0KB      0KB      N/A
Ethernet1/10         0KB      0KB      0KB      0KB      N/A
Ethernet1/11         0KB      0KB      0KB      0KB      N/A
Ethernet1/12         0KB      0KB      0KB      0KB      N/A
Ethernet1/33         0KB      0KB      0KB      0KB      N/A
Ethernet1/34         0KB      0KB      0KB      0KB      N/A
Ethernet1/35         0KB      0KB      0KB      0KB      N/A
Ethernet1/36         0KB      0KB      0KB      0KB      N/A
============================================================
Buffer Block 2       0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Avaliable = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
------------------------------------------------------------
Ethernet1/17         0KB      0KB      0KB      0KB      N/A
Ethernet1/18         0KB      0KB      0KB      0KB      N/A
Ethernet1/19         0KB      0KB      0KB      0KB      N/A
Ethernet1/20         0KB      0KB      0KB      0KB      N/A
Ethernet1/5          0KB      0KB      0KB      0KB      N/A
Ethernet1/6          0KB      0KB      0KB      0KB      N/A
Ethernet1/7          0KB      0KB      0KB      0KB      N/A
Ethernet1/8          0KB      0KB      0KB      0KB      N/A
Ethernet1/41         0KB      0KB      0KB      0KB      N/A
Ethernet1/42         0KB      0KB      0KB      0KB      N/A
Ethernet1/43         0KB      0KB      0KB      0KB      N/A
Ethernet1/44         0KB      0KB      0KB      0KB      N/A
Ethernet1/29         0KB      0KB      0KB      0KB      N/A
Ethernet1/30         0KB      0KB      0KB      0KB      N/A
Ethernet1/31         0KB      0KB      0KB      0KB      N/A
Ethernet1/32         0KB      0KB      0KB      0KB      N/A
============================================================
Buffer Block 3       0KB      0KB   5376KB   5376KB      N/A

Total Shared Buffer Avaliable = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
------------------------------------------------------------
Ethernet1/13         0KB      0KB      0KB      0KB      N/A
Ethernet1/14         0KB      0KB      0KB      0KB      N/A
```

```
Ethernet1/15          0KB       0KB       0KB       0KB       N/A
Ethernet1/16          0KB       0KB       0KB       0KB       N/A
Ethernet1/37          0KB       0KB       0KB       0KB       N/A
Ethernet1/38          0KB       0KB       0KB       0KB       N/A
Ethernet1/39          0KB       0KB       0KB       0KB       N/A
Ethernet1/40          0KB       0KB       0KB       0KB       N/A
Ethernet1/25          0KB       0KB       0KB       0KB       N/A
Ethernet1/26          0KB       0KB       0KB       0KB       N/A
Ethernet1/27          0KB       0KB       0KB       0KB       N/A
Ethernet1/28          0KB       0KB       0KB       0KB       N/A
Ethernet1/1           0KB       0KB       0KB       0KB       N/A
Ethernet1/2           0KB       0KB       0KB       0KB       N/A
Ethernet1/3           0KB       0KB       0KB       0KB       N/A
Ethernet1/4           0KB       0KB    5376KB    5376KB       N/A
```

The following example shows how to display the maximum buffer utilization information of each buffer block for multicast mode:

```
switch# show hardware profile buffer monitor brief
Brief CLI issued at: 09/18/2012 08:30:08

                   Maximum buffer utilization detected
                  1sec      5sec     60sec      5min       1hr
                 ------    ------    ------    ------    ------
Buffer Block 1        0KB       0KB       0KB       0KB       0KB

Total Shared Buffer Avaliable = 5049 Kbytes
Class Threshold Limit = 4845 Kbytes
Mcast Usage 1         0KB       0KB       0KB       0KB       0KB
============================================================
Buffer Block 2        0KB       0KB       0KB       0KB       0KB

Total Shared Buffer Avaliable = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
Mcast Usage 2         0KB       0KB       0KB       0KB       0KB
============================================================
Buffer Block 3        0KB       0KB       0KB       0KB       0KB

Total Shared Buffer Avaliable = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
Mcast Usage 3         0KB       0KB       0KB       0KB       0KB
```

The following example shows how to display detailed buffer utilization information of buffer block 3 for multicast mode:

```
switch# show hardware profile buffer monitor multicast 3 detail
Detail CLI issued at: 09/18/2012 08:30:12

Legend -
384KB  - between   1 and 384KB of shared buffer consumed by port
768KB  - between 385 and 768KB of shared buffer consumed by port
307us  - estimated max time to drain the buffer at 10Gbps

Active Buffer Monitoring for Mcast Usage 3 is: Active
KBytes                384  768 1152 1536 1920 2304 2688 3072 3456 3840 4224 4608 4992 5376 5760 6144
us @ 10Gbps           307  614  921 1228 1535 1842 2149 2456 2763 3070 3377 3684 3991 4298 4605 4912
                     ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
09/18/2012 08:30:12    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:11    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:10    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:09    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:08    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:07    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:06    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
```

```
09/18/2012 08:30:05      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:04      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 08:30:03      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
```

The following example shows how to display detailed buffer data about Ethernet interface 1/4:

```
switch# show hardware profile buffer monitor interface ethernet 1/4 detail
Detail CLI issued at: 09/18/2012 07:38:43

Legend -
384KB  - between   1 and 384KB of shared buffer consumed by port
768KB  - between 385 and 768KB of shared buffer consumed by port
307us  - estimated max time to drain the buffer at 10Gbps

Active Buffer Monitoring for port Ethernet1/4 is: Active
KBytes                 384  768 1152 1536 1920 2304 2688 3072 3456 3840 4224 4608 4992 5376 5760 6144
us @ 10Gbps            307  614  921 1228 1535 1842 2149 2456 2763 3070 3377 3684 3991 4298 4605 4912
                      ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
09/18/2012 07:38:42      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:41      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:40      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:39      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:38      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:37      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:36      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:35      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:34      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:33      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:32      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:31      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:30      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:29      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:28      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:27      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:26      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:25      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:24      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:23      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:22      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:21      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:20    177   36    0    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:19      0  143  107    0    0    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:18      0    0   72  178    3    0    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:17      0    0    0    0  176   74    0    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:16      0    0    0    0    0  105  145    0    0    0    0    0    0    0    0    0
09/18/2012 07:38:15      0    0    0    0    0    0   33  179   38    0    0    0    0    0    0    0
09/18/2012 07:38:14      0    0    0    0    0    0    0    0  140  113    0    0    0    0    0    0
09/18/2012 07:38:13      0    0    0    0    0    0    0    0    0   66  178    6    0    0    0    0
09/18/2012 07:38:12      0    0    0    0    0    0    0    0    0    0    0  173   77    0    0    0
09/18/2012 07:38:11      1    0    0    1    0    0    1    0    0    1    0    0  102   42    0    0
09/18/2012 07:38:10      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
```

Related Commands

Command	Description
[no] hardware profile buffer monitor	Enables or disables monitoring of hardware buffer data.
clear hardware profile buffer monitor	Clears the buffer of all hardware profile buffer monitor data.

show hardware profile forwarding-mode

To display the warp mode status and the host, unicast, multicast, and Layer 2 TCAM sizes, use the **show hardware profile forwarding-mode** command.

show hardware profile forwarding-mode

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the warp mode status and the host, unicast, multicast, and Layer 2 TCAM sizes.

```
switch(config)# show hardware profile forwarding-mode
switch(config)#
```

Related Commands

Command	Description
[**no**] **hardware profile forwarding-mode warp**	Enables warp mode.

show hosts

To display the Domain Name Server (DNS) name servers and domain names, use the **show hosts** command.

show hosts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the IP addresses of the DNS servers that are used to resolve hostnames:

```
switch# show hosts
```

Related Commands

Command	Description
ip domain-list	Defines a list of domains.
ip domain lookup	Enables DNS-based hostname-to-address translation.
ip domain-name	Configures a name server.

show logging console

To display the console logging configuration, use the **show logging console** command.

show logging console

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the console logging configuration:

```
switch# show logging console
```

Related Commands

Command	Description
logging console	Configures logging to the console.

show logging info

To display the logging configuration, use the **show logging info** command.

show logging info

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the logging configuration:

```
switch# show logging info
```

Related Commands

Command	Description
logging event	Logs interface events.

show logging last

To display the last number of lines of the logfile, use the **show logging last** command.

show logging last *number*

Syntax Description		
	number	Enters the number of lines to display from 1 to 9999.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

Examples This example shows how to display the last 42 lines of the log file:

```
switch# show logging last 42
```

Related Commands	Command	Description
	logging logfile	Configures the name of the log file used to store system messages.

show logging level

To display the facility logging severity level configuration, use the **show logging level** command.

show logging level [*facility*]

Syntax Description

facility	(Optional) Logging facility.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the logging severity level configuration:

```
switch# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclmgr                  3                       3
afm                     3                       3
altos                   3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
cfs                     3                       3
:

<--snip-->
:
vdc_mgr                 6                       6
vlan_mgr                2                       2
vmm                     5                       5
vshd                    5                       5
xmlma                   3                       3
zschk                   2                       2

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

This example shows how to display the EtherChannel logging severity level configuration:

```
switch# show logging level port-channel
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
eth_port_channel        5                       5

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

switch#
```

This example shows how to display the Address Resolution Protocol (ARP) logging severity level configuration:

```
switch# show logging level arp
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
arp                     2                       2

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

Related Commands

Command	Description
logging level	Configures the facility logging level.

show logging logfile

To display the messages in the log file that were timestamped within the span entered, use the **show logging logfile** command.

show logging logfile [**start-time** *yyyy mmm dd hh*:*mm*:*ss*] [**end-time** *yyyy mmm dd hh*:*mm*:*ss*]

Syntax Description

start-time *yyyy mmm dd hh*:*mm*:*ss*	(Optional) Specifies a start time in the format *yyyy mmm dd hh:mm:ss*. Use three characters for the month (*mmm*) field, digits for the year (*yyyy*) and day (*dd*) fields, and digits separated by colons for the time (*hh:mm:ss*) field.
end-time *yyyy mmm dd hh*:*mm*:*ss*	(Optional) Specifies an end time in the format *yyyy mmm dd hh:mm:ss*. Use three characters for the month (*mmm*) field, digits for the year (*yyyy*) and day (*dd*) fields, and digits separated by colons for the time (*hh:mm:ss*) field.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

If you do not enter an end time, the current time is used.

Examples

This example shows how to display the messages in the log file that were timestamped within the span shown:

```
switch# show logging logfile start-time 2008 mar 11 12:10:00
```

Related Commands

Command	Description
logging logfile	Configures logging to a log file.

show logging module

To display the module logging configuration, use the **show logging module** command.

show logging module

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the module logging configuration:

```
switch# show logging module
```

Related Commands

Command	Description
logging module	Configures module logging.

show logging monitor

To display the monitor logging configuration, use the **show logging monitor** command.

show logging monitor

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the monitor logging configuration:

```
switch# show logging monitor
```

Related Commands

Command	Description
logging monitor	Configures logging on the monitor.

show logging nvram

To display the messages in the nonvolatile random access memory (NVRAM) log, use the **show logging nvram** command.

show logging nvram [**last** *number-lines*]

Syntax Description

last *number-lines*	(Optional) Specifies the number of lines to display. The number of lines is from 1 to 100.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the last 20 messages in the NVRAM log:

```
switch# show logging nvram last 20
```

Related Commands

Command	Description
logging level	Enables logging messages from a defined facility.

show logging onboard

To display the onboard logging information based on the error type, use the **show logging onboard** command.

show logging onboard {**bcm_used** | **boot-uptime** | **device-version** | **endtime** | **environmental-history** | **exception-log** | **kernel-trace** | **obfl-history** | **obfl-logs** | **stack-trace** | **starttime** | **status** | **trident**} [> *file* | | *type*]

Syntax Description

bcm_used	Displays the onboard failure logging (OBFL) BCM usage information.
boot-uptime	Displays the OBFL boot and uptime information.
device-version	Displays the OBFL device version information.
endtime	Displays the OBFL logs until the specified end time in the following format: *mm*/*dd*/*yy*-*HH*:*MM*:*SS*
environmental-history	Displays the OBFL environmental history.
exception-log	Displays the OBFL exception log.
kernel-trace	Displays the OBFL kernel trace information.
obfl-history	Displays the OBFL history information.
obfl-logs	Displays the OBFL technical support log information.
stack-trace	Displays the OBFL kernel stack trace information.
starttime	Displays the OBFL logs from the specified start time in the following format: *mm*/*dd*/*yy*-*HH*:*MM*:*SS*
status	Displays the OBFL status enable or disable.
trident	Displays the OBFL Trident information.
> *file*	(Optional) Redirects the output to a file. See the "Usage Guidelines" section for additional information.
| *type*	(Optional) Filters the output. See the "Usage Guidelines" section for additional information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

The date and time arguments for the **starttime** and **endtime** keywords are entered as the date month/day/year (*mm*/*dd*/*yy*), followed by a hyphen, and the time in 24-hour format in hours:minutes:seconds (*HH:MM:SS*). For example:

- **starttime** 03/17/08-15:01:57

- **endtime** 03/18/08-15:04:57

The valid values for *file* are as follows:

- **bootflash:**
- **ftp:**
- **scp:**
- **sftp:**
- **tftp:**
- **volatile:**

The valid values for *type* are as follows:

- **begin** [**-i**] [**-x**] [*word*]—Begins with the line that matches the text.
  - **-i**—Ignores the case difference when comparing the strings.
  - **-x**—Prints only the lines where the match is a whole line.
  - *word*—Specifies for the expression.
- **count** [**>** *file* | **|** *type*]—Counts number of lines.
- **egrep | grep** *print-match*—Egrep or Grep. Egrep searches for lines of text that match more sophisticated regular expression syntax than grep. Grep searches for lines of text that match one or many regular expressions, and outputs only the matching lines.
  - **-A** *num*—Prints the specifies number of lines of context after every matching line. Range: 1 to 999.
  - **-B** *num*—Prints the specifies number of lines of context before every matching line. Range: 1 to 999.
  - **-c**—Prints a total count of matching lines only.
  - **-i**—Ignores the case difference when comparing the strings.
  - **-n**—Prints each match preceded by its line number.
  - **-v**—Prints only the lines that contain no matches for the *word* argument.
  - **-w**—Prints only lines where the match is a complete word.
  - **-x**—Prints only the lines where the match is a whole line.
  - *word*—Specifies for the expression.
- **exclude** [**-i**] [**-x**] [*word*]—Excludes the lines that match.
  - **-i**—Ignores the case difference when comparing the strings.
  - **-x**—Prints only the lines where the match is a whole line.
  - *word*—Specifies for the expression.
- **head** [**-n** *num*]—Stream Editor. The optional **-n** *num* keyword and argument allow you to specify the number of lines to print. Range: 0 to 2147483647.
- **include** [**-i**] [**-x**] [*word*]—Include the lines that match.
  - **-i**—Ignores the case difference when comparing the strings.
  - **-x**—Prints only the lines where the match is a whole line.
  - *word*—Specifies for the expression.

- **last** [*num*]—Displays the last lines to print. The optional *num* specifies the number of lines to print. Range: 0 to 9999.
- **less [-E | -d]**—Quits at the end of the file.
  - **-E**—(Optional) Quits at the end of the file.
  - **-d**—(Optional) Specifies a dumb terminal.
- **no-more**—Turns off pagination for command output.
- **sed** *command*—Stream Editor
- **wc**—Counts words, lines, and characters.
  - **-c**—(Optional) Specifies the output character count.
  - **-l**—(Optional) Specifies the output line count.
  - **-w**—(Optional) Specifies the output word count.
  - **>**—Redirects it to a file.
  - **|**—Pipes command output to filter.

Use this command to view OBFL data from the system hardware. The OBFL feature is enabled by default and records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with hardware cards or modules installed in a Cisco router or switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records.

The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The message “No historical data to display” is seen when historical data is not available.

Examples

This example shows how to display the OBFL boot and uptime information:

```
switch# show logging onboard boot-uptime
```

This example shows how to display the OBFL logging device information:

```
switch# show logging onboard device-version
```

This example shows how to display the OBFL history information:

```
switch# show logging onboard obfl-history
```

The **show logging onboard obfl-history** command displays the following information:

- Timestamp when OBFL is manually disabled.
- Timestamp when OBFL is manually enabled.
- Timestamp when OBFL data is manually cleared.

This example shows how to display the OBFL kernel stack trace information:

```
switch# show logging onboard stack-trace
```

The **show logging onboard stack-trace** command displays the following information:

- Time in seconds

- Time in microseconds
- Error description string
- Current process name and identification
- Kernel jiffies
- Stack trace

show logging onboard memory-errors

The **show logging onboard memory-errors** command displays the history of Parity, Single ECC, and Double ECC errors that are detected on various device memory. See the following example output for the parity errors that are detected on MAC block memory:

```
switch(config-if)# show logging onboard memory-errors
----------------------------
OBFL Data for
    Module:  1
----------------------------

:
Sun Jun 21 22:49:22 2015@665506
MEMORY::MB:: [#8] PARITY Error detected on MAC BLOCK - Interrupt
3852(MTC_MB_MAC_TBL_RAM_DLEFT_RPM1_PERR_INTR_4), Offset 0x3de, Total Errors in MAC block
106

Sun Jun 21 22:49:22 2015@665573
MEMORY::MB:: [#8] PARITY Error: RPM 1, HW entry: rpm addr 0x107de, vld 1, mac 0x300ff25,
fid 5, adj 0, rsvd 0, lid 8, lif 23, non existent 0, local 1

Sun Jun 21 22:49:22 2015@665612
MEMORY::MB:: [#8] PARITY Error: RPM 1, SW entry: index = 32232, vld 0x1, mac
0x25ff00030000, vlan 1, port 7, flags 0

Sun Jun 21 22:49:22 2015@665688
MEMORY::MB:: [#8] PARITY Error at rpm1 of bank #1, is a soft failure. MAC entry at RPM
addr 0x107de Index 32232 has been cleared.

Sun Jun 21 22:51:02 2015@671711
MEMORY::MB:: [#9] PARITY Error detected on MAC BLOCK - Interrupt
3851(MTC_MB_MAC_TBL_RAM_DLEFT_RPM0_PERR_INTR_4), Offset 0xc, Total Errors in MAC block 107

Sun Jun 21 22:51:02 2015@671803
MEMORY::MB:: [#9] PARITY Error: RPM 0, HW entry: rpm addr 0x1000c, vld 1, mac 0x300cd7e,
fid 5, adj 0, rsvd 0, lid 8, lif 23, non existent 0, local 1

Sun Jun 21 22:51:02 2015@671843
MEMORY::MB:: [#9] PARITY Error: RPM 0, SW entry: index = 200, vld 0x1, mac 0x7ecd00030000,
vlan 1, port 7, flags 0

Sun Jun 21 22:51:02 2015@671910
MEMORY::MB:: [#9] PARITY Error at rpm0 of bank #0, is a soft failure. MAC entry at RPM
addr 0x1000c Index 200 has been cleared.

Sun Jun 21 22:57:42 2015@716752
MEMORY::MB:: [#10] PARITY Error detected on MAC BLOCK - Interrupt
3788(MTC_MB_MAC_TBL_RAM_DLEFT_RPM0_PERR_INTR), Offset 0x2ee, Total Errors in MAC block 108

Sun Jun 21 22:57:42 2015@716841
MEMORY::MB:: [#10] PARITY Error: RPM 0, HW entry: rpm addr 0x2ee, vld 1, mac 0x300be27,
fid 5, adj 0, rsvd 0, lid 8, lif 23, non existent 0, local 1

Sun Jun 21 22:57:42 2015@716882
```

```
MEMORY::MB:: [#10] PARITY Error: RPM 0, SW entry: index = 12000, vld 0x1, mac
0x27be00030000, vlan 1, port 7, flags 0

Sun Jun 21 22:57:42 2015@716958
MEMORY::MB:: [#10] PARITY Error at rpm0 of bank #0, is a hard failure. MAC entry at RPM
addr 0x2ee Index 12000 has been marked invalid to prevent it from being used again
```

Related Commands

Command	Description
clear logging onboard	Clears the OBFL entries in the persistent log.
hw-module logging onboard	Enables or disabled OBFL entries based on the error type.

show logging pending

To display the pending changes to the syslog server configuration, use the **show logging pending** command.

show logging pending

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the pending changes to the syslog server configuration:

```
switch# show logging pending
```

Related Commands

Command	Description
logging abort	Cancels the pending changes to the syslog server configuration.

show logging pending-diff

To display the differences from the current syslog server configuration to the pending changes of the syslog server configuration, use the **show logging pending-diff** command.

show logging pending-diff

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the pending differences of the syslog server configuration:

```
switch# show logging pending-diff
```

Related Commands

Command	Description
logging abort	Cancels the pending changes to the syslog server configuration.

show logging session status

To display the logging session status, use the **show logging session status** command.

show logging session status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the logging session status:

```
switch# show logging session status
```

Related Commands

Command	Description
logging timestamp	Sets the logging time-stamp units.

show logging server

To display the syslog server configuration, use the **show logging server** command.

show logging server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the syslog server configuration:

```
switch# show logging server
```

Related Commands

Command	Description
logging server	Configures a remote syslog server.

show logging status

To display the logging status, use the **show logging status** command.

show logging status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the logging status:

```
switch# show logging status
```

Related Commands

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the Cisco Fabric Services (CFS) infrastructure.

show logging timestamp

To display the logging time-stamp configuration, use the **show logging timestamp** command.

show logging timestamp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the logging time-stamp configuration:

```
switch# show logging timestamp
```

Related Commands

Command	Description
logging timestamp	Configures the logging time stamp granularity.

show monitor session

To display information about the Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) sessions, use the **show monitor session** command.

show monitor session [*session* | **all** [**brief**] | **range** *range* [**brief**]]

Syntax Description

session	(Optional) Number of the session. The range is from 1 to 18.
all	(Optional) Displays all sessions.
brief	(Optional) Displays a brief summary of the information.
range *range*	(Optional) Displays a range of sessions. The range is from 1 to 18.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(2)A1(1)	This command was introduced.
6.0(2)A1(1)	Support for ERSPAN was added.

Examples

This example shows how to display information about SPAN session 1:

```
switch# show monitor session 1
session 1
---------------
description       : A Local SPAN session
type              : local
state             : down (No operational src/dst)
source intf       :
    rx            : Eth1/5
    tx            : Eth1/5
    both          : Eth1/5
source VLANs      :
    rx            :
source VSANs      :
    rx            :
destination ports : Eth1/21

Legend: f = forwarding enabled, l = learning enabled

switch#
```

This example shows how to display a range of SPAN sessions:

```
switch# show monitor session range 1-4
```

This example shows how to display the information about an ERSPAN session on a switch that runs Cisco NX-OS Release 5.0(3)U2(2):

```
switch# show monitor session 1
session 1
---------------
description       : ERSPAN source session
type              : erspan-source
state             : down (No valid global IP Address)
vrf-name          : default
destination-ip    : 192.0.2.1
ip-ttl            : 5
ip-dscp           : 3
mtu              : 1000
origin-ip         : origin-ip not specified
source intf       :
    rx            : Eth1/5
    tx            : Eth1/5
    both          : Eth1/5
source VLANs      :
    rx            :

switch#
```

Related Commands

Command	Description
monitor session	Displays the contents of the startup configuration file.
show running-config monitor	Displays the running configuration information for SPAN and ERSPAN sessions.

show ntp peer-status

To display the status of the Network Time Protocol (NTP) peers, use the **show ntp peer-status** command.

show ntp peer-status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the peer status for NTP:

```
switch# show ntp peer-status
```

Related Commands

Command	Description
show ntp peers	Displays information about NTP peers.

show ntp peers

To display information about Network Time Protocol (NTP) peers, use the **show ntp peers** command.

show ntp peers

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display information about NTP peers:

```
switch# show ntp peers
```

Related Commands

Command	Description
show ntp peer-status	Displays status information about NTP peers.

show ntp statistics

To display Network Time Protocol (NTP) statistics, use the **show ntp statistics** command.

show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** *address* | **name** *name1* [*..nameN*]}

Syntax Description

io	Displays the input-output statistics.
local	Displays the counters maintained by the local NTP.
memory	Displays the statistics counters related to the memory code.
peer	Displays the per-peer statistics counter of a peer.
ipaddr *address*	Displays statistics for the peer with the configured IPv4 address. The IPv4 address format is dotted decimal, x.x.x.x.
name *name1*	Displays statistics for a named peer.
..nameN	(Optional) Displays statistics for one or more named peers.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the statistics for NTP:

```
switch# show ntp statistics local
```

Related Commands

Command	Description
clear ntp statistics	Clears NTP statistics

show ntp timestamp-status

To display the Network Time Protocol (NTP) time-stamp information, use the **show ntp timestamp-status** command.

show ntp timestamp-status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the NTP time-stamp status:

```
switch# show ntp timestamp-status
```

Related Commands

Command	Description
ntp	Configures the NTP peers and servers.

show ptp brief

To display a brief status of the Precision Time Protocol (PTP) interfaces, use the **show ptp brief** command.

show ptp brief

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display a brief status of the PTP interfaces:

```
switch# show ptp brief

PTP port status
-----------------------
Port         State
-------  --------------
Eth1/5      Disabled
switch#
```

Related Commands

Command	Description
show ptp clock	Displays the properties of the local clock.
show ptp clock foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp corrections	Displays the last few PTP corrections.
show ptp parent	Displays the properties of the PTP parent.
show ptp port	Displays the status of the PTP port.
show ptp time-property	Displays the properties of the PTP clock.

show ptp clock

To display the Precision Time Protocol (PTP) clock information, use the **show ptp clock** command.

show ptp clock

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the PTP clock information:

```
switch# show ptp clock
PTP Device Type: Boundary clock
Clock Identity :  54:7f:ee:ff:ff: 2:47:81
Clock Domain: 1
Number of PTP ports: 0
Priority1 : 255
Priority2 : 255
Clock Quality:
        Class : 248
        Accuracy : 254
        Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Fri Sep 30 05:57:50 2011
switch#
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp corrections	Displays the last few PTP corrections.
show ptp parent	Displays the properties of the PTP parent.

Command	Description
show ptp port	Displays the status of the PTP port.
show ptp time-property	Displays the properties of the PTP clock.

show ptp clock foreign-masters-record

To display information about the state of foreign masters known to the Precision Time Protocol (PTP) process, use the **show ptp clock foreign-masters-record** command.

show ptp clock foreign-masters-record [**interface ethernet** *slot/port*]

Syntax Description

interface	(Optional) Specifies an interface.
ethernet	Specifies an IEEE 802.3z Ethernet interface.
slot/port	Slot number of the Ethernet interface. The slot number is from 1 to 255 and the port number is form 1 to 128.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the state of foreign masters known to the PTP process:

```
switch# show ptp clock foreign-masters-record
```

This example shows how to display information about the state of foreign masters known to the PTP process for the Ethernet interface 1/5:

```
switch# show ptp clock foreign-masters-record interface ethernet 1/5
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp corrections	Displays the last few PTP corrections.
show ptp parent	Displays the properties of the PTP parent.
show ptp port	Displays the status of the PTP port.
show ptp time-property	Displays the properties of the PTP clock.

show ptp corrections

To display the history of the Precision Time Protocol (PTP) clock corrections on the Ethernet interfaces, use the **show ptp corrections** command.

show ptp corrections

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the history of the PTP clock corrections on the Ethernet interfaces:

```
switch# show ptp corrections
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clock foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp parent	Displays the properties of the PTP parent.
show ptp port	Displays the status of the PTP port.
show ptp time-property	Displays the properties of the PTP clock.

show ptp parent

To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the **show ptp parent** command.

show ptp parent

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the parent and grand master of the PTP clock:

```
switch# show ptp parent

PTP PARENT PROPERTIES

Parent Clock:
Parent Clock Identity:   0: 0: 0:ff:ff: 0: 0: 0
Parent Port Number: 0
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
Grandmaster Clock Identity:   0: 0: 0:ff:ff: 0: 0: 0
Grandmaster Clock Quality:
        Class: 248
        Accuracy: 254
        Offset (log variance): 65535
        Priority1: 255
        Priority2: 255
switch#
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clock foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp corrections	Displays the last few PTP corrections.
show ptp port	Displays the status of the PTP port.
show ptp time-property	Displays the properties of the PTP clock.

show ptp port

To display information about the Precision Time Protocol (PTP) port, use the **show ptp port** command.

show ptp port interface ethernet *slot*/*port*

Syntax DescriptionT		
	interface	Specifies the interface.
	ethernet *slot*/*port*	Specifies an IEEE 802.3z Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.0(2)A1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display information about the PTP port on the Ethernet interface 1/5:

```
switch# show ptp port interface ethernet 1/5
PTP Port Dataset: Eth1/5
Port identity: clock identity:   0: 5:73:ff:ff:ff:5b: 1
Port identity: port number: 4
PTP version: 2
Port state: Disabled
VLAN info:  1
Delay request interval(log mean): 2
Peer mean path delay: 0
Announce interval(log mean): 1
Sync interval(log mean): -2
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
switch#
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clock foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp corrections	Displays the last few PTP corrections.
show ptp parent	Displays the properties of the PTP parent.
show ptp time-property	Displays the properties of the PTP clock.

show ptp time-property

To display the Precision Time Protocol (PTP) clock properties, use the **show ptp time-property** command.

show ptp time-property

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the PTP clock properties:

```
switch# show ptp time-property
PTP CLOCK TIME PROPERTY:
        Current UTC Offset valid: 0
        Current UTC Offset: 0
        Leap59: 0
        Leap61: 0
        Time Traceable: 0
        Frequency Traceable: 0
        PTP Timescale: 0
        Time Source:  0xa0(Internal Oscillator)
switch#
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clock foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp corrections	Displays the last few PTP corrections.
show ptp parent	Displays the properties of the PTP parent.
show ptp port	Displays the status of the PTP port.

show rmon

To display information about Remote Monitoring (RMON) alarms or high-capacity alarms or events, use the **show rmon** command.

show rmon {**alarms** | **events** | **hcalarms** | **info** | **logs**}

Syntax Description

alarms	Displays the RMON alarms.
events	Displays the RMON events.
hcalarms	Displays the RMON high-capacity alarms.
info	Displays the RMON configuration information.
logs	Displays information about the RMON event logs.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the RMON high-capacity alarms configured on the switch:

```
switch# show rmon hclarms
High Capacity Alarm 3 is active, owned by admin
 Monitors 1.3.6.1.2.1.2.2.1.17.83886080 every 5 second(s)
 Taking delta samples, last value was 216340
 Rising threshold is 0, assigned to event 3
 Falling threshold is 0, assigned to event 0
 On startup enable rising alarm
 Number of Failed Attempts is 0
switch#
```

This example shows how to display the RMON events configured on the switch:

```
switch# show rmon events
Event 5 is active, owned by admin
 Description is myRMONEvent
 Event firing causes nothing, last fired never
switch#
```

This example shows how to display the RMON configuration information:

```
switch# show rmon info
Maximum allowed 32 bit or 64 bit alarms : 512
Number of 32 bit alarms configured : 0
Number of 64 bit hcalarms configured : 1
switch#
```

Related Commands

Command	Description
rmon alarm	Creates RMON alarms.
rmon event	Creates RMON events.
rmon hcalarm	Creates RMON high-capacity alarms.
show running-config	Displays the running configuration.

show running-config

To display the contents of the currently running configuration file, use the **show running-config** command.

show running-config [**all**]

Syntax Description		
	all	(Optional) Displays the full operating information including default settings.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

Examples This example shows how to display information on the running configuration on a switch that runs Cisco NX-OS Release 5.0(3)A1(1):

```
switch# show running-config

!Command: show running-config
!Time: Fri May 28 10:30:02 2010

version 5.0(3)A1(1)
feature telnet
feature private-vlan

username adminbackup password 5 !  role network-operator
username admin password 5 $1$gLP0Z4.z$nA4fMnTcHmdSgQ3ENakm/1  role network-admin
ip domain-lookup
hostname switch
slot 1
snmp-server user admin network-admin auth md5 0xd727e3e4ed39de2f32841ffa24e4234c
 priv 0xd727e3e4ed39de2f32841ffa24e4234c localizedkey

vrf context management
  ip route 0.0.0.0/0 192.168.0.1
<--Output truncated-->
switch#
```

This example shows how to display detailed information on the running configuration on a switch that runs Cisco NX-OS Release 5.0(3)A1(1):

```
switch# show running-config all
```

This example shows how to display the running configuration on a switch that runs Cisco NX-OS Release 5.0(3)A1(1) and shows the Control Plane Policing (CoPP) policy maps, hardware port modes, and access control list (ACL) ternary content addressable memory (TCAM) changes:

```
switch# show running-config

!Command: show running-config
!Time: Thu Aug 25 07:39:37 2011

version 5.0(3)A1(1)
feature telnet
no feature ssh
feature lldp

username admin password 5 $1$OOV4MdOM$BAB5RkD22YanT4empqqSM0  role network-admin
ip domain-lookup
switchname switch
ip access-list my-acl
  10 deny ip any 10.0.0.1/32
  20 deny ip 10.1.1.1/32 any
class-map type control-plane match-any copp-arp
class-map type control-plane match-any copp-bpdu
class-map type control-plane match-any copp-default
class-map type control-plane match-any copp-dhcp
class-map type control-plane match-any copp-filtermatch
class-map type control-plane match-any copp-icmp
:
<--snip-->
:
class-map type control-plane match-any copp-ttl1
policy-map type control-plane copp-system-policy
  class copp-default
    police pps 400
  class copp-l2switched
    police pps 400
  class copp-icmp
    police pps 200
:
<--snip-->
control-plane
  service-policy input copp-system-policy
hardware profile tcam region arpacl 128
hardware profile tcam region ifacl 256
hardware profile tcam region racl 256
hardware profile tcam region vacl 512
hardware profile portmode 48x10G+4x40G
<--Output truncated-->
switch#
```

Related Commands

Command	Description
show startup-config	Displays the contents of the startup configuration file.

show running-config callhome

To display the Call Home running configuration, use the **show running-config callhome** command.

show running-config callhome [**all**]

Syntax Description		
	all	(Optional) Displays all the default and configured information.

Command Default Displays only the configured information.

Command Modes EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

Examples This example shows how to display the Call Home running configuration:

```
switch# show running-config callhome
```

This example shows how to display the entire Call Home running configuration, including the default values:

```
switch# show running-config callhome all
```

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.

show running-config exclude-provision

To display the running configuration without the configuration for offline preprovisioned interfaces, use the **show running-config exclude-provision** command.

show running-config exclude-provision

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the running configuration without the offline preprovisioned interfaces:

```
switch# show running-config exclude-provision

!Command: show running-config exclude-provision
!Time: Fri May 28 10:35:32 2010

version 5.0(3)A1(1)
feature telnet
feature private-vlan

username adminbackup password 5 !  role network-operator
username admin password 5 $1$gLP0Z4.z$nA4fMnTcHmdSgQ3ENakm/1  role network-admin
ip domain-lookup
hostname switch
slot 1
snmp-server user admin network-admin auth md5 0xd727e3e4ed39de2f32841ffa24e4234c
 priv 0xd727e3e4ed39de2f32841ffa24e4234c localizedkey

vrf context management
  ip route 0.0.0.0/0 192.168.0.1
vlan 1
vlan 5
  private-vlan primary
port-channel load-balance ethernet source-ip


interface Ethernet1/1
<--Output truncated-->
switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
provision	Preprovisions a module in a slot.
show provision	Displays the preprovisioned module information.
show startup-config exclude-provision	Displays the startup configuration without the preprovisioning information for offline interfaces.
slot	Configures a chassis slot for a predefined module.

show running-config interface

To display the running configuration information for interfaces, use the **show running-config interface** command.

show running-config interface [**all** | **ethernet** *slot/port* | **loopback** *if_number* | **mgmt** *mgmt_intf* | **port-channel** *po_number*]

Syntax Description

all	(Optional) Displays all the default and configured information.
ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
mgmt *mgmt_intf*	Specifies the management interface. The interface number is 0.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.

Command Default

Displays only the configured information.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the running configuration for a specified Ethernet interface on a switch that runs Cisco NX-OS Release 5.0(3)A1(1):

```
switch# show running-config interface ethernet 1/5

!Command: show running-config interface Ethernet1/5
!Time: Fri Aug 26 04:12:01 2011

version 5.0(3)A1(1)

interface Ethernet1/5
  speed auto

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration information to the startup configuration file.

show running-config monitor

To display the running configuration for the Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **show running-config monitor** command.

show running-config monitor [**all**]

Syntax Description

all	(Optional) Displays current SPAN configuration information including default settings.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(2)A1(1)	This command was introduced.
6.0(2)A1(1)	Support for ERSPAN was added.

Examples

This example shows how to display information on the running SPAN and ERSPAN configuration:

```
switch# show running-config monitor

!Command: show running-config monitor
!Time: Wed Sep 28 19:11:41 2011

version 5.0(3)U2(2)
monitor session 1 type erspan-source
  description ERSPAN source session
  vrf default
  destination ip 192.0.2.1
  ip ttl 5
  ip dscp 3
  source interface Ethernet1/5 both
  mtu 1000
  no shut
monitor session 3 type erspan-destination
  description ERSPAN destination session
  source ip 192.0.1.1
  destination interface Ethernet1/2

switch#
```

This example shows how to display detailed information on the running SPAN and ERSPAN configuration:

```
switch# show running-config monitor all
```

Related Commands

Command	Description
monitor session	Configures SPAN or ERSPAN sessions.
show monitor session	Displays information about SPAN or ERSPAN sessions.

show scheduler

To display information about the scheduled maintenance jobs, use the **show scheduler** command.

show scheduler {**config** | [**mem-stats**] | **job** [**name** *jobname*] | **logfile** | **schedule** [**name** *schedulename*]}

Syntax Description

config	Displays the scheduler configuration information.
mem-stats	(Optional) Provides the scheduler internal memory information as specified.
job	Displays the job information as specified.
name *jobname*	(Optional) Displays information for the specified scheduler job name. The job name can be any alphanumeric string up to 31 characters.
logfile	Displays the scheduler log file as specified.
schedule	Displays the scheduler timetable as specified.
name *schedulename*	(Optional) Displays the scheduler timetable for the specified schedule name. The schedule name can be any alphanumeric string up to 31 characters.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the scheduler configuration:

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 16
end

switch#
```

Related Commands

Command	Description
scheduler	Configures maintenance jobs.
feature scheduler	Enables the scheduler feature for scheduling maintenance jobs.

show snmp community

To display the Simple Network Management Protocol (SNMP) community strings configured on the switch, use the **show snmp community** command.

show snmp community

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP community strings:

```
switch# show snmp community
```

Related Commands

Command	Description
snmp-server community	Configures the community access string to permit access to the SNMP protocol.

show snmp context

To display the Simple Network Management Protocol (SNMP) contexts configured on the switch, use the **show snmp context** command.

show snmp context

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP contexts:

```
switch# show snmp context
```

Related Commands

Command	Description
snmp-server context	Configures an SNMP context.

show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine, use the **show snmp engineID** command.

show snmp engineID

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a local or remote device. SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine.

Examples

This example shows how to display the SNMP engine ID:

```
switch# show snmp engineID
```

Related Commands

Command	Description
show running-config	Displays the running system configuration information.
snmp-server user	Configures a new user to a SNMP group.

show snmp group

To display the names of the Simple Network Management Protocol (SNMP) groups configured on the switch, use the **show snmp group** command.

show snmp group

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP groups:

```
switch# show snmp group
```

Related Commands

Command	Description
show running-config	Displays the running system configuration information.

show snmp host

To display the Simple Network Management Protocol (SNMP) host information, use the **show snmp host** command.

show snmp host

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP host:

```
switch# show snmp host
```

Related Commands

Command	Description
snmp-server host	Configures an SNMP host.

show snmp sessions

To display the current Simple Network Management Protocol (SNMP) sessions, use the **show snmp sessions** command.

show snmp sessions

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP sessions:

```
switch# show snmp sessions
```

Related Commands

Command	Description
show running-config	Displays the running system configuration information.

show snmp trap

To display the Simple Network Management Protocol (SNMP) link trap generation information, use the **show snmp trap** command.

show snmp trap

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP traps:

```
switch# show snmp trap
```

Related Commands

Command	Description
snmp trap link-status	Enables SNMP link trap generation.

show snmp user

To display information on each Simple Network Management Protocol (SNMP) user, use the **show snmp user** command.

show snmp user

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the SNMP users configured on the switch:

```
switch# show snmp user
```

This example shows how to display information about a specific SNMP user:

```
switch# show snmp user admin
```

Related Commands

Command	Description
snmp-server user	Configures a new user to an SNMP group.

show startup-config

To display the contents of the currently running configuration file, use the **show startup-config** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display information from the startup configuration file:

```
switch# show startup-config

!Command: show startup-config
!Time: Fri May 28 11:05:41 2010
!Startup config saved at: Fri May 28 11:05:35 2010

version 5.0(3)A1(1)
feature telnet
feature private-vlan

username adminbackup password 5 !  role network-operator
username admin password 5 $1$gLP0Z4.z$nA4fMnTcHmdSgQ3ENakm/1  role network-admin
ip domain-lookup
hostname switch
slot 1
snmp-server user admin network-admin auth md5 0xd727e3e4ed39de2f32841ffa24e4234c
 priv 0xd727e3e4ed39de2f32841ffa24e4234c localizedkey
<--Output truncated-->
switch#
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file.

show startup-config callhome

To display the startup configuration for Call Home, use the **show startup-config callhome** command.

show startup-config callhome

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the startup configuration for Call Home:

```
switch# show startup-config callhome
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

show startup-config exclude-provision

To display the startup configuration that excludes the configuration for offline preprovisioned interfaces, use the **show startup-config exclude-provision** command.

show startup-config exclude-provision

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the startup configuration without the offline preprovisioned interfaces:

```
switch# show startup-config exclude-provision
```

Related Commands

Command	Description
provision	Preprovisions a module in a slot.
show provision	Displays the preprovisioned module information.
show running-config exclude-provision	Displays the running configuration excluding the preprovisioned features.
slot	Configures a chassis slot for a predefined module.

show startup-config ptp

To display the Precision Time Protocol (PTP) startup configuration, use the **show startup-config ptp** command.

show startup-config ptp [**all**]

Syntax Description		
	all	(Optional) Displays all the default and configured information.

Command Default Displays only the configured information.

Command Modes EXEC mode

Command History	Release	Modification
	6.0(2)A1(1)	This command was introduced.

Examples This example shows how to display the PTP startup configuration:

```
switch# show startup-config ptp

!Command: show startup-config ptp
!Time: Wed Mar 13 08:10:00 2013
!Startup config saved at: Wed Mar 13 08:09:56 2013

version 6.0(2)A1(1)
feature ptp

ptp domain 1
ptp source 192.0.2.1
ptp priority1 10
ptp priority2 20


interface Ethernet1/5
  ptp
  ptp vlan 5
  ptp delay-request minimum interval 2

switch#
```

This example shows how to display the entire PTP startup configuration, including the default values:

```
switch# show startup-config ptp all
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration information to the startup configuration file.
ptp source	Configures the global source IP for PTP packets.

show startup-config vtp

To display the VLAN Trunking Protocol (VTP) configuration from the startup configuration file, use the **show startup-config vtp** command.

show startup-config vtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the VTP configuration stored in the startup configuration file:

```
switch# show startup-config vtp
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration file.
feature vtp	Enables VTP on the switch.
vtp domain	Configures the VTP administrative domain.
vtp file	Stores the VTP configuration in a file.
vtp mode	Configures a VTP device mode.

show tech-support callhome

To display the technical support output for Call Home, use the **show tech-support callhome** command.

show tech-support callhome

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to display the troubleshooting information for Call Home:

```
switch# show tech-support callhome
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.
show running-config callhome	Displays the running configuration information for Call Home.

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
6.0(2)A1(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.

site-id (Call Home)

To configure the optional site number for the customer, use the **site-id** command. To remove a site number, use the **no** form of this command.

site-id *site-number*

no site-id

Syntax Description

site-number	Site number. The site number can be up to 255 alphanumeric characters in free format.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

You can configure the customer identification information that Cisco Smart Call Home should use. The service agreement includes the customer identification information, such as the customer ID, contract ID, and site ID.

Examples

This example shows how to configure a site number:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# site-id 10020-1203
switch(config-callhome)#
```

Related Commands

Command	Description
switch-priority	Configures the switch priority for the switch.
show callhome	Displays a summary of the Call Home 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
5.0(3)A1(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 3548 Switch NX-OS Security Configuration Guide* for more information on creating ACLs. The ACL applies to IPv4 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# configure terminal
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
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to set an SNMP contact:

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

This example shows how to remove an SNMP contact:

```
switch# configure terminal
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
5.0(3)A1(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# configure terminal
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** | **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** | **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.
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
5.0(3)A1(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# configure terminal
switch(config)# snmp-server enable traps aaa
switch(config)#
```

This example shows how to disable all SNMP notifications:

```
switch# configure terminal
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
5.0(3)A1(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# configure terminal
switch(config)# snmp-server enable traps link
switch(config)#
```

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

```
switch# configure terminal
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 enable traps vtp

To enable the Simple Network Management Protocol (SNMP) notifications for a VLAN Trunking Protocol (VTP) domain, use the **snmp-server enable traps vtp** command. To disable SNMP notifications on a VTP domain, use the **no** form of this command.

snmp-server enable traps vtp

no snmp-server enable traps vtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(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.

This command does not require a license.

Examples

This example shows how to enable SNMP notifications on a VTP domain:

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

This example shows how to disable all SNMP notifications on a VTP domain:

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

Related Commands

Command	Description
show snmp trap	Displays the SNMP notifications enabled or disabled.
show vtp status	Displays VTP information.

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
5.0(3)A1(1)	This command was introduced.

Examples

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

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

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

```
switch# configure terminal
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	Name or Internet address of the 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
5.0(3)A1(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# configure terminal
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# configure terminal
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
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to set a system location string:

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

This example shows how to remove the system location string:

```
switch# configure terminal
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
5.0(3)A1(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# configure terminal
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# configure terminal
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.

Command	Description
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
5.0(3)A1(1)	This command was introduced.

Examples

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

```
switch# configure terminal
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# configure terminal
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) 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
5.0(3)A1(1)	This command was introduced.

Examples

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

```
switch# configure terminal
```

```
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# configure terminal
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

Command History

Release	Modification
5.0(3)A1(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.

Examples

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

```
switch# configure terminal
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# configure terminal
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# configure terminal
```

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

Related Commands

Command	Description
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*/*port* | **port-channel** *channel-num*} [{**both** | **rx** | **tx**}] | **vlan** *vlan-num*}

no source {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-num*} | **vlan** *vlan-num*}

Syntax Description

interface	Specifies the interface type to use as the source SPAN port.
ethernet *slot*/*port*	Specifies the IEEE 802.3z Ethernet interface to use as the source SPAN port. The slot number is from 1 to 255 and the port number is from 1 to 128.
port-channel *channel-num*	Specifies the EtherChannel interface to use as the source SPAN port. The EtherChannel number is from 1 to 4096.
both	(Optional) Specifies both ingress and egress traffic on the source port. **Note** Applies to ERSPAN source port.
rx	(Optional) Specifies only ingress traffic on the source port. **Note** Applies to ERSPAN source port.
tx	(Optional) Specifies only egress traffic on the source port. **Note** Applies to 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.

Command Default

None

Command Modes

SPAN session configuration mode
ERSPAN session configuration mode

Command History

Release	Modification
6.0(2)1A(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, or a VLAN 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.

source ip (ERSPAN)

To configure the source IP address for an an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination, use the **source ip** command. To remove the source IP configuration, use the **no** form of this command.

source ip *ip_address*

no source ip *ip_address*

Syntax Description

ip_address	IP address for the ERSPAN session.

Command Default

None

Command Modes

ERSPAN destination configuration mode

Command History

Release	Modification
6.0(2)1A(1)	This command was introduced.

Usage Guidelines

An ERSPAN destination session supports only one source IP address.

Examples

This example shows how to configure a source IP address for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-destination
switch(config-erspan-dst)# source ip 192.0.2.1
switch(config-erspan-dst)#
```

Related Commands

Command	Description
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.

streetaddress (Call Home)

To configure the street address for the primary person responsible for the switch, use the **streetaddress** command. To remove the street address, use the **no** form of this command.

streetaddress *address*

no streetaddress

Syntax Description

address	Street address. The address can be a maximum of 255 alphanumeric characters and can include white spaces.

Command Default

None

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure the street address for the primary person responsible for the switch:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# streetaddress 170 West Tasman Drive, San Jose, CA 95134-1706
switch(config-callhome)#
```

Related Commands

Command	Description
contract-id	Configures the contract number for the switch.
copy running-config startup-config	Saves this configuration change.
show callhome	Displays a summary of the Call Home configuration.

switch-priority (Call Home)

To configure the switch priority for the switch, use the **switch-priority** command. To remove the switch priority, use the **no** form of this command.

switch-priority *priority-value*

no switch-priority

Syntax Description

priority-value	Switch priority value. The range is from 0 to 7, with 0 being the highest priority and 7 the lowest.

Command Default

Default priority is 7

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure the switch priority:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# switch-priority 5
switch(config-callhome)#
```

Related Commands

Command	Description
show callhome	Displays a summary of the Call Home configuration.

tag

To correlate multiple events in the policy, use the **tag** command.

tag *tag* {**and | andnot | or**} *tag* [**and | andnot | or** {**tag**}]{**happens** occurs **in** *seconds*}

Syntax Descriptiona

tag	Tag name. The tag name can be any alphanumeric string up to 29 characters.
and	(Optional) Specifies to use boolean and logic.
andnot	(Optional) Specifies to use boolean andnot logic.
or	(Optional) Specifies to use boolean or logic.
happens	Specifies the number of occurrences before raising the event.
occurs	Number of times that the event occurs. The range is from 1 to 4294967295.
in	Specifies the number of occurrences that must occur within this time period.
seconds	Time in seconds that the next event occurs. The range is from 0 to 4294967295 seconds.

Defaults

None

Command Modes

Applet configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to correlate multiple events in the policy:

```
switch# configuration terminal
switch(config)# event manager applet monitorShutdown
switch(config-applet)# description "Monitors interface shutdown."
switch(config-applet)# event cli match "shutdown"
switch(config-applet)# tag one or two happens 1 in 10000
switch(config-applet)# action 1.0 cli show interface ethernet 3/1
```

Related Commands

Command	Description
description	Configures a descriptive string for the policy.
event	Configures the event statement for the policy.
show event-manager policy state	Displays information about the status of the configured policy.

terminal event-manager bypass

To specify the command-line interface (CLI) events that match the Embedded Event Manager (EEM) policies to bypass the EEM events, use the **terminal event-manager bypass** command.

terminal event-manager bypass

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the command-line interface (CLI) events that match the Embedded Event Manager (EEM) policies to bypass the EEM events:

```
switch# configure terminal
switch(config)# terminal event-manager bypass
switch(config)#
```

Related Commands

Command	Description
action event-default	Specifies that the default action for the event is to be performed when an EEM applet is triggered.

transport email (Call Home)

To configure the Simple Mail Transport Protocol (SMTP) server address for the Call Home functionality to work, and optionally the from and reply-to e-mail addresses, use the **transport email** command. To remove the SMTP server, use the **no** form of this command.

transport email {**from** *email-addr* | **mail-server** *ip-address* [**port** *port-no*] [**priority** *priority-no*] | **reply-to** *email-addr* | **smtp-server** *ip-address* [**port** *port-no*] [**use-vrf** *vrf-name*]}

no transport email {**from** | **mail-server** *ip-address* [**port** *port-no*] [**priority** *priority-no*] | **reply-to** | **smtp-server**}

Syntax Description

from	Specifies the e-mail from field for Call Home messages.
email-addr	E-mail address. The address can be a maximum of 255 alphanumeric characters and cannot include white spaces; for example, *personname@companyname.com*.
mail-server	Configures the SMTP server address for supporting multiple SMTP servers.
ip-address	Domain name server (DNS) name, IPv4 address of the SMTP server.
port *port-no*	(Optional) Specifies the SMTP server port. The port number range is from 1 to 65535, and the default port number is 25.
priority *priority-no*	(Optional) Specifies the SMTP server priority. The server priority value range is from 1 to 100, and the default is 50.
reply-to	Specifies the reply-to email address.
smtp-server	Configures the SMTP server address.
use-vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding instance (VRF) instance to use when communicating with this SMTP server. The name is case sensitive and has 255 alphanumeric characters.

Command Default

SMTP port number: 25

SMTP server priority: 50

Command Modes

Callhome configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to configure the SMTP server for the Call Home service:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)#
```

This example shows how to configure the e-mail from and reply-to field for Call Home messages:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# transport email from person@example.com
switch(config-callhome)# transport email reply-to person@example.com
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.
show callhome transport-email	Displays information about the e-mail configuration for Call Home.
transport email	Configures the SMTP server address for Call Home.

verify (session)

To verify the current configuration session, use the **verify** command.

verify

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Session configuration mode

Command History

Release	Modification
5.0(3)A1(1)	This command was introduced.

Examples

This example shows how to verify a session:

```
switch# configure session MySession
switch(config-s)# verify
Failed to start Verification: Session Database already locked, Verify/Commit in
Progress.
switch(config-s)#
```

Related Commands

Command	Description
commit	Commits a session.
configure session	Creates a configuration session.
show configuration session	Displays the contents of the session.

vrf (ERSPAN)

To configure a virtual routing and forwarding (VRF) instance for Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic forwarding in the source, use the **vrf** command. To revert to the default settings, use the **no** form of this command.

vrf {*vrf_name* | **default** | **management**}

no vrf {*vrf_name* | **default** | **management**}

Syntax Description

vrf_name	Name of the VRF. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
default	Specifies the default VRF instance.
management	Specifies the management VRF instance.

Command Default

None

Command Modes

ERSPAN session configuration mode

Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a VRF instance for the ESRSPAN source:

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

Related Commands

Command	Description
monitor-session	Enters the monitor configuration mode for configuring an ERSPAN session for analyzing traffic between ports.
show monitor session	Displays information about the Ethernet Switched Port Analyzer (SPAN) or ERSPAN monitor session.