Cisco Nexus 5500 Series NX-OS System Management Command Reference

First Published: 2016-04-22

Last Modified: 2022-02-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface

This preface describes the audience, organization, and conventions of the Book Title. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS on Cisco Nexus 5000 Series Platform switches.

Document Conventions

Note

- As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.
- The Guidelines and Limitations section contains general guidelines and limitations that are applicable to all the features, and the feature-specific guidelines and limitations that are applicable only to the corresponding feature.

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.

Convention	Description
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information 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 Cisco Nexus 5000 Series Switches is available at:

- Configuration Guides

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-and-configuration-guides-list.html

- Command Reference Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-command-reference-list.html

- Release Notes

  http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-release-notes-list.html

- Install and Upgrade Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html

- Licensing Guide

  http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-licensing-information-listing.html

Documentation for Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at:

http://www.cisco.com/c/en/us/support/switches/nexus-2000-series-fabric-extenders/products-installation-and-configuration-guides-list.html

Documentation Feedback

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

A Commands

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
5.2(1)N1(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.

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
	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.

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
	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.

acllog match-log-level

To specify the minimum severity level to log ACL matches, use the acllog match-log-level command. To remove the acllog match log level, use the no form of this command.

acllog match-log-level severity-level
no acllog match-log-level severity-level

Syntax Description

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 • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition—default level • 6—informational: Informational message only (default) • 7—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set the acllog match-log-level to 6, informational:

```
switch(config)# acllog match-log-level 6
switch(config)#
```

Related Commands

Command	Description
logging level	Enables logging messages from a specified facility and configures the logging severity level.
logging logfile	Configures the name of the log file used to store system messages and sets the minimum severity level to log.

C Commands

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
	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(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.

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
	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(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.

configure maintenance profile

To enter a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile, use the configure maintenance profile command. To delete the existing maintenance mode profile or normal mode profile, use the no form of this command. Starting with Cisco NX-OS Release 7.3(0)N1(1), we recommend not using the configure profile [maintenance-mode | normal-mode] type admin command and we strongly recommend using the configure maintenance profile [maintenance-mode | normal-mode] command.

configure maintenance profile [maintenance-mode | normal-mode]
no configure maintenance profile [maintenance-mode | normal-mode]

Syntax Description

maintenance-mode	Enters the maintenance profile configuration session for a maintenance mode profile.
normal-mode	Enters the maintenance profile configuration session for a normal mode profile.

Command Default

None

Command Modes

Privileged EXEC (#)

Global configuration mode (config)

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enter a maintenance profile configuration session for a maintenance mode profile:

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)#
```

This example shows how to enter a maintenance profile configuration session for a normal mode profile:

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)#
```

This example shows how to delete a maintenance profile:

```
switch# no configure maintenance profile maintenance-mode
Maintenance mode profile maintenance-mode successfully deleted
Enter configuration commands, one per line. End with CNTL/Z.
Exit maintenance profile mode.
```

Related Commands

Command	Description
show run mmode	Displays the currently running maintenance profile configuration on a switch.
show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
system mode maintenance always-use-custom-profile	Applies the existing custom maintenance-mode profile and prevents creation of auto-generated maintenance-mode profile.
system mode maintenance on-reload reset-reason	Boots the switch into maintenance-mode automatically in the event of a specified system crash.
system mode maintenance shutdown	Shuts down all protocols and interfaces except the management interface (by using the shutdown command and not the default isolate command).
system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

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

Examples

This example shows how to commit the current session:

```
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.

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
	This command was introduced.

Examples

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

```
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.

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

Examples

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

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

Related Commands

Command	Description
show ntp	Displays NTP information.

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
5.2(1)N1(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
```

Related Commands

Command	Description
show ntp	Displays NTP information.

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

Examples

This example shows how to clear the current logging session:

```
switch# clear logging session
```

Related Commands

Command	Description
show logging session	Displays the logging session status.

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

Examples

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

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

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

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

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

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

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

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

Related Commands

Command	Description
show logging onboard	Displays onboard failure logs.

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

Examples

This example shows how to clear the NVRAM logs:

```
switch# clear logging nvram
```

Related Commands

Command	Description
show logging nvram	Displays the NVRAM logs.

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
5.2(1)N1(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.

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
	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.

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
	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(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

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
	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(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).

D Commands

destination-profile (Call Home)

To create a user-defined destination profile, or modify a predefined or user-defined destination profile, and 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
	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 5000 Series 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 lists each Call Home message level keyword.

Table 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(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.

destination (SPAN session)

To configure a Switched Port Analyzer (SPAN) destination port, use the destination command. To remove the destination SPAN port, use the no form of this command.

destination interface ethernet slot/[QSFP-module/] port | port-channel channel-num | vlan vlan-num | vsan vsan-num
no destination interface ethernet slot/[QSFP-module/] port | port-channel channel-num | vlan vlan-num | vsan vsan-num

Syntax Description

interface	Specifies the interface type to use as the destination SPAN port.
ethernet slot/[QSFP-module/] port	Specifies the Ethernet interface to use as the destination SPAN port. The slot number is from 1 to 255. The QSFP-module number is from 1 to 4. The port number is from 1 to 128. **Note** The QSFP-module number applies only to the QSFP+ Generic Expansion Module (GEM).
port-channel channel-num	Specifies the EtherChannel interface to use as the destination SPAN port. The EtherChannel number is from 1 to 4096.
vlan vlan-num	Specifies the VLAN interface to use as the destination SPAN port. The range is from 1 to 3967 and 4048 to 4093.
vsan vsan-num	Specifies the virtual storage area network (VSAN) to use as the destination SPAN port. The range is from 1 to 4093.

Command Default

None

Command Modes

SPAN session configuration mode

Command History

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

Usage Guidelines

Each local SPAN session destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source port.

The destination port can be any Ethernet physical port and must reside on the same switch as the source port (for a local SPAN session). The destination port cannot be a source port, a port channel, or SAN port channel group.

A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.

Examples

This example shows how to configure an Ethernet interface SPAN destination port and activate the SPAN session:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport monitor
switch(config-if)# exit

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 1/5
switch(config-monitor)# no shutdown
switch(config-monitor)#
```

Related Commands

Command	Description
source (SPAN session)	Configures a source 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.

destination (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	Configures the remote IP address.
ip_address	IPv4 address in the format A .B .C .D .

Command Default

None

Command Modes

ERSPAN session configuration mode

Command History

Release	Modification
5.2(1)N1(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 or VSAN interface.

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 modeERSPAN session configuration mode

Command History

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

Usage Guidelines

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

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.

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

Examples

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

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

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

```
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.

E Commands

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
	This command was introduced.

Examples

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

```
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
	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(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(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.

F Commands

factory reset

To remove all the identifiable customer information on Cisco NX-OS devices in conditions of productremoval due to Return Merchandise Authorization (RMA), or upgrade or replacement, or system end-of- life you can use the factory-reset command to securely erase all information.

Note There is no form of this command, once deleted you cannot regain the deleted information.

factory-reset fex-id | <all>

Command History

fex id	Securely erase fex as per identifier number. The range is 100-199.
all	Securely erase all the fex.
factory-reset	Securely erase data on the switch.

Command History

Release	Modification
7.3(11)N1(1)	This command was introduced.

Usage Guidelines

Youuse this command to erase customer information.

This command does not require a license.

Note If fex is attached to the switch, to erase the customer data on the connected fex perform below operation before performing a factory reset on the switch:

- To erase customer data on a single fex - factory reset fex <fex-id>
- To erase customer data on all fex - factory reset all

Examples

This example shows the factory-reset of a switch:

```
switch(config)# factory-reset
!!!! WARNING !!!!

The factory reset operation will erase ALL persistent storage on the specified module.
This includes configuration, all log data, and the full contents of flash and SSDs.
Special steps are taken in an effort to render data non-recoverable. Please, proceed with
caution and understanding that this operation cannot be undone and will leave the system
in a fresh-from-factory state.

!!!! WARNING !!!!
Continue? (y/n) [n] y
```

```
A device reload is required for the reset operation to proceed.
Please, wait...
WARNING: This command will reboot the system
2006 Apr 24 06:23:17 switch %$ VDC-1 %$ %PFMA-2-PFM_SYSTEM_RESET: Manual system restart
from Command Line Interface
[ 972.939186] Shutdown Ports..
[ 972.947864] writing reset reason 9,
Secure erase requested! Please, do not power off module!
```

feature ptp

To enable the PTP feature, use the feature ptp command. To unconfigure the PTP feature, use the no form of this command.

feature ptp
no feature ptp

Syntax Description

There are no arguments or keywords for this command.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to enable PTP on the device:

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

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 priority 1 value to use when advertising this clock.
ptp priority2	Configures the priority 1 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

filter access-group

To apply an access group to an Encapsulated Remote Switched Port Analyzer (ERSPAN) or Switched Port Analyzer (SPAN) source session, use the filter access-group command. To remove an access group, use the no form of this command.

filter access-group acl-filter
no filter access-group acl-filter

Syntax Description

acl-filter	Access control list (ACL) name. An ACL associates the access list with the SPAN session.

Command Default

None

Command Modes

SPAN session configuration mode (config-monitor)ERSPAN source session configuration mode (config-erspan-src)

Command History

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

Usage Guidelines

ACL filtering allows you to filter SPAN and ERSPAN traffic so that you can reduce bandwidth congestion. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in the spanning of traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter applies to all sources in the session.

Note If the ACL has rules with a log option configured, the log option is ignored but the rule is implemented.

Examples

This example shows how to enable an ACL filter for a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# filter access-group acl_span_ses_3
```

This example shows how to enable an ACL filter for a ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 4 type erspan-source
switch(config-erspan-src)# filter access-group acl_erspan_ses_3
```

Related Commands

Command	Description
monitor session	Creates a new SPAN or ERSPAN session.

fex-group

To create a Fabric Extender (FEX) group, use the fex-group command. To delete a FEX group., use the no form of this command.

fex-group name
no fex-group name

Syntax Description

name	Specifies the name of the FEX group.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create a FEX group “fg1”:

```
switch# fex-group fg1
```

This example shows how to delete a FEX group “fg1”:

```
switch# no fex-group fg1
```

Related Commands

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

Command	Description
system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.
Command	Description

I Commands

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
5.2(1)N1(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 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 long.
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
5.2(1)N1(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.

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 modeVRF context configuration mode

Command History

Release	Modification
5.2(1)N1(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# config 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
```

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

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

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# config 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
```

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

Usage Guidelines

Use the ip host command to add a static hostname to DNS.

Examples

This example shows how to configure a static hostname:

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

Related Commands

Command	Description
ipv6 host	Configures a static host name in the DNS database.
show hosts	Displays information about the IP domain name configuration.

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 modeVRF context configuration mode

Command History

Release	Modification
5.2(1)N1(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# config 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# config 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# config terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
```

Related Commands

Command	Description
ip domain-list	Configures the IP domain list.

Command	Description
ip domain-lookup	Enables the Domain Name Server (DNS) lookup feature.
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
5.2(1)N1(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# config 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-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-list	Specifies the 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 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 modeVRF context configuration mode

Command History

Release	Modification
5.2(1)N1(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# config terminal
switch(config)# ip domain-list Mysite.com
```

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

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

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# config 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
```

Related Commands

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

ip dns source-interface

To configure the source interface for the Domain Name Server (DNS) domain lookup, use the ip dns source-interface command. To revert to the default settings, use the no form of this command.

ip dns source-interface ethernet slot /[QSFP-module/] port | loopback intf-num [vrf vrf-name | default | management]
no ip dns source-interface ethernet slot /[QSFP-module/] port | loopback intf-num [vrf vrf-name | default | management]

Syntax Description

ethernet slot /[QSFP-module/] port	Specifies the Ethernet interface to use as the source interface. The slot number is from 1 to 255. The QSFP-module number is from 1 to 4. The port number is from 1 to 128. **Note** The QSFP-module number applies only to the QSFP+ Generic Expansion Module (GEM).
loopback intf-num	Specifies the loopback interface to use as the source interface. The range of values is from 0 to 1023.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name. The name is case sensitive and can be a maximum of 32 characters.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an Ethernet interface as the source interface for a DNS lookup:

```
switch# configure terminal
switch(config)# ip dns source-interface ethernet 1/5
switch(config)#
```

Related Commands

Command	Description
ip domain-lookup	Enables the DNS lookup feature.
show ip dns source-interface	Displays information about the DNS source interfaces.

L Commands

locator-led

To turn on the locator LED of a Fabric Extender, use the locator-led command. To turn off the locator LED, use the no form of this command.

locator-led chassis pattern long | medium | short | fex fex_number

no locator-led chassis pattern long | medium | short | fex fex_number

Syntax Description

chassis	Specifies the Blink chassis LED.
pattern	Specifies the LED blink pattern.
long	Specifies a long LED blink.
medium	Specifies a medium LED blink.
short	Specifies a short LED blink.
fex_number	Fabric Extender number. The range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the locator-led command to toggle the locator LED of a Fabric Extender, which allows you to easily identify the machine in a busy data center.

Example

This example shows how to turn on the locator LED for a specific Fabric Extender chassis:

```
switch# locator-led fex 100
switch#
```

This example shows how to turn off the locator beacon LED for a specific Fabric Extender chassis:

```
switch# no locator-led fex 100
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show locator-led	Displays the status of the locator LED in Fabric Extender modules.

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

Examples

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

```
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 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
5.2(1)N1(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(config)# logging timestamp microseconds
```

Related Commands

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

logging server

To configure a remote syslog server at the specified hostname or IPv4/IPv6 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 auth | authpriv | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user | uucp | use-vrf vrf_name | management]
no logging server host [severity-level] [facility auth | authpriv | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user | uucp | use-vrf vrf_name | management]

Syntax Description

host	Hostname or IPv4/IPv6 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 facilities are listed in Table 1-1 of Appendix 1, "System Message Logging Facilities." 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
5.2(1)N1(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(config)# logging server 192.168.2.253
```

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

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

Related Commands

Command	Description
show logging server	Displays the configured syslog servers.

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
5.2(1)N1(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(config)# logging monitor
```

Related Commands

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

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
5.2(1)N1(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(config)# logging module
```

Related Commands

Command	Description
show logging module	Displays the module logging status.

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
5.2(1)N1(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(config)# logging logfile logfile 4
```

Related Commands

Command	Description
show logging logfile	Displays the log file.

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. The facilities are listed in Table 1-1 of Appendix 1, "System Message Logging Facilities." 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
5.2(1)N1(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(config)# logging level aaa 2
```

Related Commands

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

logging ip access-list cache

To configure the Optimized ACL Logging (OAL) parameters, use the logging ip access-list cache command. To reset to the default settings, use the no form of this command.

logging ip access-list cache entries num_entries | interval seconds | threshold num_packets
no logging ip access-list cache entries num_entries | interval seconds | threshold num_packets

Syntax Description

entries num_entries	Specifies the maximum number of log entries that are cached in the software. The range is from 0 to 1048576. The default value is 8000 entries.
interval seconds	Specifies the maximum time interval before an entry is sent to a syslog. The range is from 5 to 86400. The default value is 300 seconds.
threshold num_packets	Specifies the number of packet matches (hits) before an entry is sent to a syslog. The range is from 0 to 1000000. The default value is 0 packets—rate limiting is off; the system log is not triggered by the number of packet matches.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the maximum number of log entries that are cached in the software:

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 200
switch(config)#
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
switch# configure terminal
switch(config)# logging ip access-list cache interval 350
switch(config)#
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
switch# configure terminal
switch(config)# logging ip access-list cache threshold 125
switch(config)#
```

Related Commands

Command	Description
show logging ip access-list	Displays the status of IP access list logging.

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
5.2(1)N1(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
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.
show logging	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 port link-status | trunk-status default | enable
no logging event port 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

Command History

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

Examples

This example shows how to log interface events:

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

Related Commands

Command	Description
show logging	Displays the logging status.

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

Examples

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

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

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

```
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 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
5.2(1)N1(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
```

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

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

Examples

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

```
switch(config)# logging distribute
switch(config)# 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.

M Commands

monitor erspan origin ip-address

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) origin IP address, use the monitor espan origin ip-address command. To remove the ERSPAN 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 virtual device context (VDC) configuration across all VDCs.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to configure the ERSPAN 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 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.

mtu

To configure the maximum transmission unit (MTU) truncation size for packets in the specified Ethernet Switched Port Analyzer (SPAN) session, use the mtu command. To remove the MTU truncation size configuration, use the no form of this command.

mtu mtu-size
no mtu

Syntax Description

mtu-size	MTU truncation size. The range is from 64 to 1500.

Command Default

Disabled

Command Modes

Monitor configuration (config-monitor)

Command History

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

Usage Guidelines

MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration.

Note MTU truncation is supported only on F1 Series modules and F2 Series modules.

This command does not require a license.

Examples

This example shows how to configure the MTU truncation size for packets in the specified SPAN session:

```
switch# configure terminal
switch(config)# monitor session 5
switch(config-monitor)# mtu 128
switch(config-monitor)#
```

This example shows how to remove the MTU truncation size configuration for packets in the specified SPAN session:

```
switch# configure terminal
switch(config)# monitor session 5
switch(config-monitor)# no mtu
```

Related Commands

Command	Description
monitor session	Places you in the monitor configuration mode for configuring a SPAN session.

Command	Description
show monitor session	Displays the status of the SPAN session.

monitor session

To create a new Ethernet 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 or ERSPAN sessions, use the no form of this command.

monitor session session-number [shut] | type local | 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-source	Creates an ERSPAN source session.
suspend	(Optional) Specifies to suspend the referenced SPAN session.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(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.

Note The Cisco Nexus 6000 switch supports two active SPAN sessions. The Cisco Nexus 5548 Switch supports four active SPAN sessions. When you configure more than two SPAN sessions, the first two sessions are active. During startup, the order of active sessions is reversed; the last two sessions are active. For example, if you configured ten sessions 1 to 10 where 1 and 2 are active, after a reboot, sessions 9 and 10 will be active. To enable deterministic behavior, explicitly suspend the sessions 3 to 10 with the monitor session session-number shut command.

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

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(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
```

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

```
switch(config)# interface ethernet 1/2

switch(config-if)# switchport

switch(config-if)# switchport monitor

switch(config-if)# no shutdown
```

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

```
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
```

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.
erspan-id (ERSPAN)	Sets the flow ID for an ERSPAN session.

Command	Description
ip dscp (ERSPAN)	Sets the DSCP value for an ERSPAN packet.
ip prec (ERSPAN)	Sets the IP precedence 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.

N Commands

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
5.2(1)N1(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(config)# ntp server ntp.cisco.com
```

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

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

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

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

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
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
5.2(1)N1(1)	This command was introduced.

Examples

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

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

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
5.2(1)N1(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(config)# ntp distribute
```

Related Commands

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

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

Examples

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

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

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 command to allow synchronization with unauthenticated, unconfirmed network peers.

ntp authenticate
no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode (config)

Command History

Release	Modification
5.2(1)N1(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.

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the switchto vdc command.

This command does not require a license.

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.

Examples

This example shows how to enable NTP authentication:

```
switch# config terminal
```

switch(config)# ntp authenticate

This example shows how to disable NTP authentication:

```
switch(config)# no
 ntp authenticate
switch(config)#
```

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

Examples

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

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

Related Commands

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

P Commands

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

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

```
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.

ptp vlan

To specify the VLAN for the interface where PTP is being enabled, use the ptp vlan command. To disable this feature, use the no form of this command.

ptp vlan vlan-id
no ptp vlan

Syntax Description

vlan-id	The VLAN ID for the interface where PTP is being enabled. The range is from 1 to 4094.

Command Default

1

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

PTP can only be enabled on one VLAN on an interface.

Examples

This example shows how to specify VLAN 10 as the interface where PTP is being enabled:

```
switch# configure terminal
switch(config) # interface ethernet
 5/1
switch(config-if) # ptp vlan 10
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
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.
show ptp brief	Displays the PTP status.
show ptp port interface ethernet	Displays the status of the PTP port on the switch.

ptp sync interval

To configure the interval between PTP synchronization messages, use the ptp sync interval command. To disable this feature, use the no form of this command.

ptp sync interval log-seconds
no ptp sync interval

Syntax Description

log-seconds	The number of log seconds between PTP synchronization messages on an interface. The range is from -3 seconds to 1 second.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Examples

This example shows how to set the PTP synchronization interval to -3:

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

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
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 VLAN for the interface where PTP is being enabled.
show ptp brief	Displays the PTP status.
show ptp port interface ethernet	Displays the status of the PTP port on the switch.

ptp source

To configure the source IP address for all PTP packets, use the ptp source command. To unconfigure the source IP address for all PTP packets, use the no form of this command.

ptp source ip-address [vrf vrf]
no ptp source ip-address [vrf vrf]

Syntax Description

sip-address	Specifies the source IP address for all PTP packets. The IP address can be in IPv4 or IPv6 format.
vrf vrf	Specifies the VRF.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

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

```
switch(config)# ptp source 192.0.2.1
```

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 priority 1 value to use when advertising this clock.
ptp priority2	Configures the priority 1 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 to use when advertising this clock, use the ptp priority2 command.

ptp priority2 value
no ptp priority2 value

Syntax Description

value	The configured value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.

Command Default

255 when advertising the clock

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set the priority2 value used to advertise this clock:

```
switch(config)# ptp priority2 20
```

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 priority1

To configure the priority1 value to use when advertising this clock, use the ptp priority1 command.

ptp priority1 value
no ptp priority1 value

Syntax Description

value	The configured value overrides the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. The range is from 0 to 255.

Command Default

255 when advertising the clock

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set the priority1 value used to advertise this clock:

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

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 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 domain

To configure the domain number to use for this clock, use the ptp domain command. PTP domains allow you touse multiple independent PTP clocking subdomains on a single network.

ptp domain number
no ptp domain number

Syntax Description

number	Configures the domain number to use for this clock. The range is from 0 to 128.

Command Default

0

Command Modes

Global configuration mode

Command History

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

Examples

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

```
switch(config)# ptp domain 1
```

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 priority1	Configures the priority 1 value to use when advertising this clock.
ptp priority2	Configures the priority 1 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 delay request minimum interval

To configure the minimum interval allowed between PTP delay request messages when the port is in the master state, use the ptp delay request minimum interval command. To disable this feature, use the no form of this command.

ptp delay request minimum interval log-seconds
no ptp delay request minimum interval

Syntax Description

log-seconds	The number of log seconds between PTP delay request messages. The range is from -1 to 6 seconds.

Command Default

0 log seconds

Command Modes

Interface configuration mode

Command History

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

Examples

This example shows how to set the minimum delay request interval to 3:

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

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
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 sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the VLAN for the interface where PTP is being enabled.
show ptp brief	Displays the PTP status.
show ptp port interface ethernet	Displays the status of the PTP port on the switch.

ptp announce

To configure the interval between PTP announcement messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the ptp announce command. To disable this feature, use the no form of this command.

ptp announce interval log-seconds | timeout count
no ptp announce

Syntax Description

interval log-seconds	The number of log seconds between PTP announcement messages. The range is from 0 to 4 seconds.
timeout count	The number of PTP intervals before a timeout occurs on the interface. The range is from 2 to 10.

Command Default

The default interval is 1 log second.

The default timeout is 3 announce intervals.

Command Modes

Interfaces configuration mode

Command History

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

Examples

This example shows how to set the announcement interval on interface 5/1 to 1:

```
switch# configure terminal
switch(config) # interface ethernet
 5/1
switch(config-if)# ptp announce interval 1
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 sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the VLAN for the interface where PTP is being enabled.
show ptp brief	Displays the PTP status.
show ptp port interface ethernet	Displays the status of the PTP port on the switch.

poweroff module

To power off a module, use the poweroff module command. To return power to the module, use the no form of this command.

poweroff module module
no poweroff module module

Syntax Description

module	Module number. The range is from 1 to 18.

Command Default

None

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to power off module 2:

```
switch# poweroff module 2
```

Related Commands

Command	Description
show module	Displays information about modules.

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
	This command was introduced.

Examples

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

```
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.

R Commands

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
	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 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.
ownername	(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
	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 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 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(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.

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

S Commands

snmp-server enable traps link

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

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

Syntax Description

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

Command Default

Disabled

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

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

Examples

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

```
switch(config)# snmp-server enable tra
ps link
switch(config)#
```

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

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

Related Commands

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

snmp-server enable traps

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

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

Syntax Description

aaa	(Optional) Enables notifications for a AAA server state change.
server-state-change	(Optional) Specifies the AAA server state change.
callhome	(Optional) Enables Cisco Call Home notifications.
event-notify	(Optional) Specifies the Cisco Call Home external event notification.
smtp-send-fail	(Optional) Specifies the SMTP message send fail notification.
entity	(Optional) Enables notifications for a change in the module status, fan status, or power status.
entity_fan_status_change	(Optional) Specifies the entity fan status change.
entity_mib_change	(Optional) Specifies the entity MIB change.
entity_module_inserted	(Optional) Specifies the entity module inserted.
entity_module_removed	(Optional) Specifies the entity module removed.
entity_module_status_change	(Optional) Specifies the entity module status change.
entity_power_out_change	(Optional) Specifies the entity power out change.
entity_power_status_change	(Optional) Specifies the entity power status change.
entity_unrecognised_module	(Optional) Specifies the entity unrecognized module.
fcdomain	(Optional) Enables notifications for the Fibre Channel domain.

fcns	(Optional) Enables notifications for the name server.
fcs	(Optional) Enables notifications for the fabric configuration server.
fctrace	(Optional) Enables notifications for the route to an N port.
fspf	(Optional) Enables notifications for the Fabric Shortest Path First (FSPF).
license	(Optional) Enables notifications for the license manager.
notify-license-expiry	(Optional) Specifies the license expiry notification.
notify-license-expiry-warning	(Optional) Specifies the license expiry warning notification.
notify-licensefile-missing	(Optional) Specifies the license file missing notification.
notify-no-license-for-feature	(Optional) Specifies that a notification is sent when no license needs to be installed for the feature.
link	(Optional) Enables notifications for uplink and downlink interfaces.
rf	(Optional) Enables notifications for the redundancy framework.
redundancy_framework	(Optional) Specifies the Redundancy_Framework (RF) supervisor switchover MIB.
rmon	(Optional) Enables notifications for rising, falling, and high-capacity alarms.
fallingAlarm	(Optional) Specifies the RMON falling alarm.
hcFallingAlarm	(Optional) Specifies the high-capacity RMON falling alarm.
hcRisingAlarm	(Optional) Specifies the high-capacity RMON rising alarm.
risingAlarm	(Optional) Specifies the RMON rising alarm.
rscn	(Optional) Enables RSCN notifications.
snmp	(Optional) Enables SNMP authentication notifications.
authentication	(Optional) Specifies the SNMP authentication trap.
vsan	(Optional) Enables notifications for VSANs.
vtp	(Optional) Enables notifications for a VLAN Trunking Protocol (VTP) domain.
zone	(Optional) Enables zone notifications.
default-zone-behavior-change	(Optional) Specifies the default zone behavior change notification.
merge-failure	(Optional) Specifies the merge failure notification.
merge-success	(Optional) Specifies the merge success notification.
request-reject1	(Optional) Specifies the request reject notification.

unsupp-mem	(Optional) Specifies the unsupported member notification.

Command Default

All notifications

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

switch(config)#
```

This example shows how to disable all SNMP notifications:

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

Related Commands

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

snmp-server context

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

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

Syntax Description

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

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

snmp-server contact

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

snmp-server contact [text]
no snmp-server contact [text]

Syntax Description

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

Command Default

No system contact (sysContact) string is set.

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set an SNMP contact:

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

This example shows how to remove an SNMP contact:

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

Related Commands

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

snmp-server community

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

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

Syntax Description

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

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
show snmp community	Displays the SNMP community strings.

snmp 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 modeVirtual Ethernet interface configuration mode

Command History

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

Usage Guidelines

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

You can use this command on the following interfaces:

- Layer 2 interface
- Layer 3 interface

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

- Virtual Ethernet interface

Examples

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

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

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

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

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

```
switch(config)# interface ethernet 1/1

switch(config-if)# snmp trap link-status

switch(config-if)#
```

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

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

Related Commands

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

snapshot section

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

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

Syntax Description

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

Command Default

None.

Command History

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

Usage Guidelines

This command does not require a license.

Examples

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

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

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

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

snapshot delete

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

snapshot delete allsnapshot-name

Syntax Description

all	Deletes all the snapshots in the system.
snapshot-name	Deletes the specified snapshot.

Command Default

None

Command History

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

Usage Guidelines

This command does not require a license.

Examples

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

```
switch# snapshot delete all
```

This example shows how to delete a specific snapshot:

```
switch # snapshot delete snapshot1
```

Related Commands

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

snapshot create

To create a snapshot, use the snapshot create command.

snapshot create name description

Syntax Description

name	The name variable can be 64 characters in length.
description	The description variable can be 256 characters in length.

Command Default

None.

Command History

Release	Modification
7.1.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create a snapshot:

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

Related Commands

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

sleep instance

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

sleep instance instance-number seconds
no sleep instance instance-number seconds

Syntax Description

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

Command Default

None

Command Modes

maintenance profile configuration (config-mm-profile)

Command History

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

Examples

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

```
switch#
configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)#
interface ethernet 1/1
switch(config-mm-profile-if-verify)#
no shutdown

switch(config-mm-profile-if-verify)#
exit
switch(config-mm-profile)#
sleep instance 1 20
switch(config-mm-profile)#
router bgp 200
switch(config-mm-profile-router)#
address-family ipv4 unicast
switch(config-mm-profile-router-af)#
redistribute direct route-map my-rmap-deny
switch(config-mm-profile-router-af)#
exit

switch(config-mm-profile-router)#
exit
```

```
switch(config-mm-profile)#
sleep instance 1 10
```

Related Commands

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

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
	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(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.

shut (ERSPAN)

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

shut
no shut

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

ERSPAN session configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to shut down an ERSPAN session:

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

This example shows how to enable an ERSPAN session:

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

Related Commands

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

system fex-group shutdown

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

system fex-group name shutdown
no system fex-group name shutdown

Syntax Description

name	Specifies the name of the FEX group.

Command Default

None

Command Modes

Maintenance profile configuration (config-mm-mode)

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to shutdown a FEX group:

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

This example shows how to bring up a FEX group:

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

Related Commands

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

system mode maintenance timeout

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

system mode maintenance timeout value
no system mode maintenance timeout value

Syntax Description

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

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

This command does not require a license.

Examples

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

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

Related Commands

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

system mode maintenance shutdown

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

system mode maintenance shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command does not require a license.

Examples

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

```
switch# configure terminal
switch(config)# system mode maintenance shutdown
Following configuration will be applied:
router bgp 100
  shutdown
router ospf 100
  shutdown
router isis 100
  shutdown
system interface shutdown
Do you want to continue (y/n)? [no] y
Generating a snapshot before going into maintenance mode
Starting to apply commands...
Applying : router bgp 100
Applying :   shutdown
Applying : router ospf 100
Applying :   shutdown
Applying : router isis 100
Applying :   shutdown
Applying : system interface shutdown
Maintenance mode operation successful.
```

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
show run mmode	Displays the currently running maintenance profile configuration on a switch.

Command	Description
show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.
system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

system mode maintenance on-reload reset-reason

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

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

Syntax Description

reason	Specifies the reset reason. The reset reasons are as follows: • HW_ERROR—Hardware error • SVC_FAILURE—Critical service failure • KERN_FAILURE—Kernel panic • WDOG_TIMEOUT—Watchdog timeout • FATAL_ERROR—Fatal error • MANUAL_RELOAD---Manual reload • MAINTENANCE—Reloads the switch in maintenance mode if the switch was already in maintenance mode before reload. • MATCH_ANY—Any of the above reasons • ANY_OTHER—Any reload reason not specified above

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.

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

system mode maintenance dont-generate-profile

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

system mode maintenance dont-generate-profile
no system mode maintenance dont-generate-profile

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command does not require a license.

Examples

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

```
switch(config)# system mode maintenance dont-generate-profile
Following configuration will be applied:
router bgp 100
  isolate
sleep instance 1 10
interface Ethernet1/1
  shutdown
Do you want to continue (y/n)? [no] y
Generating a snapshot before going into maintenance mode
Starting to apply commands...
Applying : router bgp 100
Applying :   isolate
Applying : sleep instance 1 10
Applying : interface Ethernet1/1
Applying :   shutdown
Maintenance mode operation successful.
```

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
show run mmode	Displays the currently running maintenance profile configuration on a switch.

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

system mode maintenance always-use-custom-profile

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

system mode maintenance always-use-custom-profile

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode (config)

Command History

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

Usage Guidelines

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

This command does not require a license.

Examples

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

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

Related Commands

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

system mode maintenance

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

system mode maintenance
no system mode maintenance

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

This command does not require a license.

Examples

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

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:
router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate
Do you want to continue (y/n)? [no] y
Generating a snapshot before going into maintenance mode
Starting to apply commands...
Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate
Maintenance mode operation successful.
```

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

```
switch# configure terminal
switch(config)# no system mode maintenance
Following configuration will be applied:
router isis 100
  no isolate
router ospf 100
  no isolate
router bgp 100
  no isolate
Do you want to continue (y/n)? [no] y
Starting to apply commands...
Applying : router isis 100
Applying :   no isolate
Applying : router ospf 100
Applying :   no isolate
Applying : router bgp 100
Applying :   no isolate
Maintenance mode operation successful.
Generating Current Snapshot
Please use 'show snapshots compare before_maintenance after_maintenance' to check the health
 of the system
```

Related Commands

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

system soft-reload enable

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

system soft-reload enable
no system soft-reload enable

Syntax Description

This command has no arguments or keywords.

Command Default

Soft reload is disabled.

Command Modes

Global configuration mode (config)

Command History

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

Usage Guidelines

This command does not require a license.

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

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

Examples

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

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

This example shows how to disable soft reload:

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

Related Commands

Command	Description
show system soft-reload status	Displays the status of the soft reload.

Command	Description
soft-reload	Performs a manual soft reload of the switch.

switch-profile

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

switch-profile sw-profile-name
no switch-profile sw-profile-name all-config | local-config | profile-only

Syntax Description

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

Command Default

None

Command Modes

Configuration synchronization mode

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

Peer A

```
switch# configure terminal

switch(config)# cfs ipv4 distribute

switch(config)# exit

switch# config sync

Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile s5010

Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

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

Peer B

```
switch# configure terminal

switch(config)# cfs ipv4 distribute

switch(config)# exit

switch# config sync

Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile s5010

Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

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

Peer A

```
switch# config sync

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

Related Commands

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

switchport monitor rate-limit

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

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

- Cisco Nexus 5010 Series
- Cisco Nexus 5020 Series

This command does not require a license.

Examples

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

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

Related Commands

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

source (SPAN, ERSPAN)

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

source interface ethernet slot /[QSFP-module/] port | port-channel channel-num | vethernet veth-num [both | rx | tx] | vlan vlan-num | vsan vsan-num
no source interface ethernet slot /[QSFP-module/] port | port-channel channel-num | vethernet veth-num [both | rx | tx] | vlan vlan-num | vsan vsan-num

Syntax Description

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

Command Default

None

Command Modes

SPAN session configuration modeERSPAN session configuration mode

Command History

Release	Modification
6.0(2)N1(2)	Support for the QSFP+ GEM was added.

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

switch(config-monitor)#
```

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

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

Related Commands

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

snmp-server aaa-user cache-timeout

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

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

Syntax Description

seconds	Timeout value, in seconds. The range is from 1 to 86400. The default value is 3600 seconds.

Command Default

3600 seconds.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the AAA user synchronization timeout value:

```
switch(config)# snmp-server aaa-user cache-timeout 6000
```

Related Commands

Command	Description
show snmp	Displays information about SNMP.

snmp-server user

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

snmp-server user username [groupname] [auth md5 | sha auth-password [engineID engine-ID | localizedkey | priv priv-password | aes-128]]
no snmp-server user

Syntax Description

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

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

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

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

switch(config)#
```

This example shows how to delete an SNMP user:

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

Related Commands

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

snmp-server tcp-session

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

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

Syntax Description

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

Command Default

Disabled

Command Modes

Global configuration mode

Command History

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

Examples

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

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

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

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

Related Commands

Command	Description
show snmp	Displays the SNMP status.

snmp-server mib community-map

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

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

Syntax Description

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

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

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

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

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

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

Related Commands

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

snmp-server location

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

snmp-server location [text]
no snmp-server location [text]

Syntax Description

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

Command Default

No system location string is set.

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set a system location string:

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

This example shows how to remove the system location string:

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

Related Commands

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

snmp-server host

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

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

Syntax Description

host-address	IPv4 or IPv6 address or DNS name of the SNMP notification host.
community-string	String sent with the notification operation. The string can be a maximum of 32 alphanumeric characters. We recommend that you define this string using the snmp-server community command prior to using the snmp-server host command.
filter-vrf vrf-name	Specifies the virtual routing and forwarding (VRF) instance. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.
informs	Sends SNMP informs to this host.
traps	Sends SNMP traps to this host.

version	Specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the priv keyword. If you use the version keyword, one of the following must be specified:
	• 1—SNMPv1.
	• 2c—SNMPv2C.
	• 3—SNMPv3. The following three optional keywords can follow the version 3 keyword:
	  • auth—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
	  • noauth (Default)—The noAuthNoPriv security level. This is the default if the auth, noauth, or priv keyword is not specified.
	  • priv—Enables Data Encryption Standard (DES) packet encryption (also called "privacy")

udp-port port	(Optional) Specifies the UDP port of the host to use. The port range is from 0 to 65535.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

switch(config)# snmp-server host 192.168.0.10
my_acl_for_public

switch(config)#
```

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

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

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

switch(config)#
```

Related Commands

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

snmp-server globalEnforcePriv

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

snmp-server globalEnforcePriv
no snmp-server globalEnforcePriv

Syntax Description

This command has no arguments or keywords.

Command Default

The SNMP agent accepts SNMPv3 messages without authentication and encryption.

Command Modes

Global configuration mode

Command History

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

Examples

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

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

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

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

Related Commands

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

soft-reload

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

soft-reload

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command does not require a license.

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

Examples

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

```
switch# soft-reload
```

Related Commands

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

Show Commands

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
	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 destination-profile

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

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

Syntax Description

profile	(Optional) Displays information about a specific destination profile.
CiscoTAC-1	(Optional) Show 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
	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
email addresses configured:
url addresses configured:
alert groups configured:
all
CiscoTAC-1 destination profile information
maximum message size:5000000
message format:XML
```

```
message-level:0
transport-method:email
email addresses configured:
url addresses configured:
alert groups configured:
cisco-tac
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

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 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
	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 tech-support mmode

To display information for maintenance profile troubleshooting, use the show tech-support mmode command.

show tech-support mmode

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for maintenance profile troubleshooting:

```
switch# show tech-support mmode
`show system mode`
System Mode: Normal
`show maintenance profile`
[Normal Mode]
router bgp 100
  no isolate
[Maintenance Mode]
router bgp 100
  isolate
`show maintenance on-reload reset-reasons`
Reset reasons for on-reload maintenance mode:
---------------------------------------------
(not configured)
bitmap = 0x0
`show maintenance timeout`
Maintenance mode timeout value: 0 minutes
`show system internal mmode mem-stats`
Num blocks     User size     Total size    Library
--------------------------------------------------------------------------------
      16              560           800  mmode
     265            51818         55824  ld-2.8.so
       1               20            32  libdl-2.8.so
       1               38            56  libpthread-2.8.so
      12             2860          3056  libsviifdb.so.0.0.0
```

Related Commands

Command	Description
system mode maintenance always-use-custom-profile	Applies the existing custom maintenance-mode profile and prevents creation of auto-generated maintenance-mode profile.

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

show system mode

To display the current system mode, use the show system mode command. Starting with Cisco NX-OS Release 7.3(0)N1(1), you can use the show system mode command to also display the current state of the maintenance mode timer when the switch is in maintenance mode

show system mode

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
7.3(0)N1(1)	Supports display of current state of the maintenance mode timer when the switch is in maintenance mode.
7.1.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the current system mode:

```
switch# show system mode

System Mode : Normal
```

This example shows how to display the current system mode and the state of the maintenance mode timer when the switch is in maintenance mode:

```
switch# show system mode

System Mode: Maintenance
Maintenance Mode Timer: 24 minutes 55 seconds remaining
```

This example shows that the switch is in maintenance mode and that the maintenance mode timer is not running:

```
switch#  show   system   mode

System Mode: Maintenance
Maintenance Mode Timer: not running
```

Related Commands

Command	Description
show run mmode	Displays the currently running maintenance profile configuration on a switch.

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

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

Examples

This example shows how to display the SNMP users configured on the switch:

```
switch# show snmp user

_____________________________________________________________________
                    SNMP USERS
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  ____________  ______
admin                           md5   des(no)       network-admin
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv
____                            ____  ____
switch#
```

This example shows how to display information about a specific SNMP user:

```
switch# show snmp user admin

switch#
```

Related Commands

Command	Description
snmp-server user	Configures a new user to an SNMP group.

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

Examples

This example shows how to display the SNMP traps:

```
switch# show snmp trap

--------------------------------------------------------------------------------
Trap type                         Description                    Enabled
--------------------------------------------------------------------------------
entity               : entity_mib_change                           Yes
entity               : entity_module_status_change                 Yes
entity               : entity_power_status_change                  Yes
entity               : entity_module_inserted                      Yes
entity               : entity_module_removed                       Yes
entity               : entity_unrecognised_module                  Yes
entity               : entity_fan_status_change                    Yes
link                 : linkDown                                    Yes
link                 : linkUp                                      Yes
link                 : IETF-extended-linkDown                      Yes
link                 : IETF-extended-linkUp                        Yes
link                 : cisco-extended-linkDown                     Yes
link                 : cisco-extended-linkUp                       Yes
callhome             : event-notify                                No
callhome             : smtp-send-fail                              No
cfs                  : state-change-notif                          No
cfs                  : merge-failure                               No
rf                   : redundancy_framework                        Yes
aaa                  : server-state-change                         No
license              : notify-license-expiry                       Yes
license              : notify-no-license-for-feature               Yes
license              : notify-licensefile-missing                  Yes
license              : notify-license-expiry-warning               Yes
zone                 : unsupp-mem                                  No
upgrade              : UpgradeOpNotifyOnCompletion                 Yes
upgrade              : UpgradeJobStatusNotify                      Yes
feature-control      : FeatureOpStatusChange                       No
sysmgr               : cseFailSwCoreNotifyExtended                 No
rmon                 : risingAlarm                                 No
rmon                 : fallingAlarm                                No
```

```
rmon                : hcRisingAlarm                          No
rmon                : hcFallingAlarm                         No
config              : ccmCLIRunningConfigChanged             No
snmp                : authentication                         No
bridge              : topologychange                         No
bridge              : newroot                                No
stp                 : inconsistency                          No
stpx                : loop-inconsistency                     No
stpx                : root-inconsistency                     No
switch#
```

Related Commands

Command	Description
snmp trap link-status	Enables SNMP link trap generation.

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
5.2(1)N1(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 snmp	Displays the running configuration information about SNMP.

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

Examples

This example shows how to display the SNMP groups:

```
switch# show snmp group

Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write
Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read
Role: vdc-admin
  Description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write
Role: vdc-operator
  Description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read
Role: priv-3
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
```

```
  Vrf policy: permit (default)
Role: priv-2
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
Role: priv-1
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
Role: priv-0
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  10      permit  command                         traceroute6 *
  9       permit  command                         traceroute *
  8       permit  command                         telnet6 *
  7       permit  command                         telnet *
  6       permit  command                         ping6 *
  5       permit  command                         ping *
  4       permit  command                         ssh6 *
  3       permit  command                         ssh *
  2       permit  command                         enable *
  1       permit  read
Role: priv-15
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read-write
switch#
```

Related Commands

Command	Description
show running-config snmp	Displays the running configuration information about SNMP.

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
5.2(1)N1(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

Local SNMP engineID: [Hex] 8000000903000DECB230C0
                     [Dec] 128:000:000:009:003:000:013:236:178:048:192
switch#
```

Related Commands

Command	Description
show running-config snmp	Displays the running configuration information about SNMP.

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

Examples

This example shows how to display the SNMP community strings:

```
switch# show snmp community

Community            Group / Access      context    acl_filter
---------            --------------      -------    ----------
public                network-admin
switch#
```

Related Commands

Command	Description
snmp-server community	Configures the community access string to permit access to the SNMP protocol.

show snapshots sections

To display the user-specified sections in a snapshot, use the show snapshots sections command.

show snapshots sections

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the user-specified sections in a snapshot:

```
switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[v4route]
show command: show ip route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

Related Commands

Command	Description
show snapshots compare	Displays the comparison between two snapshots.
show snapshots dump	Displays content of the various sections in a generated snapshot.
snapshot create name description	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
snapshot delete	Deletes a snapshot.
snapshot section	Adds or deletes a snapshot section.

show snapshots dump

To display content of the various sections in a generated snapshot, use the show snapshots dump command.

show snapshots dump snapshot-name

Syntax Description

snapshot-name	Name of the snapshot.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to display content of the various sections in a generated snapshot:

```
switch# show snapshots dump new

File:  interface.xml        Snapshot:  new
================================================================================
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.N1.1.:if_manager">
 <nf:data>
  <show>
   <interface>
    <__readonly__>
     <TABLE_interface>
      <ROW_interface>
       <interface>mgmt0</interface>
       <state>up</state>
       <admin_state>up</admin_state>
       <eth_hw_desc>GigabitEthernet</eth_hw_desc>
       <eth_hw_addr>5cfc.666d.3b34</eth_hw_addr>
       <eth_bia_addr>5cfc.666d.3b34</eth_bia_addr>
       <eth_ip_addr>5.24.100.101</eth_ip_addr>
       <eth_ip_mask>16</eth_ip_mask>
       <eth_ip_prefix>5.24.0.0</eth_ip_prefix>
       <eth_mtu>1500</eth_mtu>
```

Related Commands

Command	Description
show snapshots	Displays snapshots on a switch.
show snapshots sections	Displays content of the various sections in a generated snapshot.

Command	Description
snapshot create name description	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
snapshot delete	Deletes a snapshot.
show snapshots dump	Displays content of the various sections in a generated snapshot.
snapshot section	Adds or deletes a snapshot section.

show snapshots compare

To display the comparison between the two snapshots on a switch, use the show snapshots compare command.

show snapshots snapshot-1 snapshot-2 [ipv4routes | ipv6routes | summary]

Syntax Description

snapshot-1 snapshot-2	Displays the comparison between the two snapshots.
ipv4routes	Displays a comparison of the IPv4 routes between the two snapshots.
ipv6routes	Displays a comparison of the IPv6 routes between the two snapshots.
summary	Displays a summary of the comparison between the two snapshots.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
7.1.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display a comparison between two snapshots:

```
switch# show snapshots compare before_maint during_maint

================================================================================
Feature              Tag                 before_maint       during_maint
================================================================================

[bgp]
--------------------------------------------------------------------------------

[eigrp]
--------------------------------------------------------------------------------

[eigrpv6]
--------------------------------------------------------------------------------

[interface]
--------------------------------------------------------------------------------

... <snip> ...

[v4route]
--------------------------------------------------------------------------------

        [ipprefix:0.0.0.0/32]
```

```
                    uptime                PT24M32S            **PT58M37S**

        [ipprefix:127.0.0.0/8]
                    uptime                PT24M32S            **PT58M37S**
```

This example shows how to display a summary of the comparison between two snapshots:

```
switch# show snapshots compare before_maintenance after_maintenance summary

================================================================================
Feature                        before_maintenance after_maintenance
changed
================================================================================
basic summary
   # of interfaces                            50              50
   # of vlans                                 0               0
   # of ipv4 routes  vrf default              13              13
   # of ipv4 paths   vrf default              13              13
   # of ipv4 routes  vrf management           14              14
   # of ipv4 paths   vrf management           14              14
   # of ipv6 routes  vrf default              3               3
   # of ipv6 paths   vrf default              3               3
interfaces
   # of eth interfaces                        48              48
   # of eth interfaces up                     1               1
   # of eth interfaces down                   47              47
   # of eth interfaces other                  0               0
   # of vlan interfaces                       0               0
   # of vlan interfaces up                    0               0
   # of vlan interfaces down                  0               0
   # of vlan interfaces other                 0               0
```

This example shows how to display a comparison of the IPv4 routes between the two snapshots:

```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
```

Related Commands

Command	Description
show snapshots	Displays snapshots on a switch.
show snapshots dump	Display content of the various sections in a generated snapshot.
show snapshots sections	Displays content of the various sections in a generated snapshot.
snapshot create name description	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
snapshot delete	Deletes a snapshot.
show snapshots dump	Displays content of the various sections in a generated snapshot.
snapshot section	Adds or deletes a snapshot section.

show snapshots

To display the snapshots present on the switch, use the show snapshots command.

show snapshots

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
7.1.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the snapshots present on the switch:

```
switch# show snapshots
Snapshot Name           Time                            Description
---------------------------------------------------------------------------
before_maintenance      Wed May 13 13:21:16 1970   system-internal-snapshot
new                     Mon May 11 15:51:27 1970       after if down
```

Note In the above output example, “before_Maintenance” is the system-generated snapshot and “new” is the user-generated snapshot.

Related Commands

Command	Description
snapshot create name description	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
snapshot delete	Deletes a snapshot.
show snapshots compare	Displays the comparison between two snapshots.
show snapshots dump	Displays content of the various sections in a generated snapshot.
snapshot section	Adds or deletes a snapshot section.

show running-config port-security

To display the running system configuration information about secure ports, use the show running-config port-security command.

show running-config port-security [all]

Syntax Description

all	(Optional) Displays detailed information about secure ports, including default settings.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the running system configuration of all secure ports on an interface:

```
switch# show running-config port-security
!Command: show running-config port-security
!Time: Tue Apr 12 10:06:56 2005
version 5.2(1)N1(1)
feature port-security
interface Ethernet1/5
  switchport port-security
  switchport port-security aging time 3
  switchport port-security maximum 10
  switchport port-security mac-address sticky
switch#
```

Related Commands

Command	Description
clear port-security dynamic	Clears the dynamically secured addresses on a port.
show startup-config port-security	Displays the configuration information in the startup file.

show running-config poe

[NOTE: per Christine, “the commands exist in the software but I was told they will remain in the code but we shouldn't show them in the docs until the rubicon fex goes out”]

To display the running configuration for Power over Ethernet (PoE) ports, use the show running-config poe command.

show running-config poe [all]

Syntax Description

all	(Optional) Displays detailed information about PoE ports, including default settings.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)N2(1)	This command was introduced.

Examples

This example shows how to display the running configuration for PoE ports:

```
switch# show running-config poe
```

Related Commands

Command	Description
show startup-config poe	Displays the startup configuration information about PoE ports.
show tech-support poe	Displays troubleshooting information about PoE ports.

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

Examples

This example shows how to display information on the running SPAN configuration:

```
switch# show running-config monitor

!Command: show running-config monitor
!Time: Thu Jan  1 06:48:56 2009
version 5.2(1)N1(1)
monitor session 1
  description A Local SPAN session
  source interface Ethernet1/5 both
  destination interface Ethernet1/21
  no shut
switch#
```

This example shows how to display detailed information on the running SPAN configuration:

```
switch# show running-config monitor all

!Command: show running-config monitor all
!Time: Thu Jan  1 06:51:08 2009
version 5.2(1)N1(1)
monitor session 1 type local
  description A Local SPAN session
  source interface Ethernet1/5 both
  destination interface Ethernet1/21
  no shut
switch#
```

Related Commands

Command	Description
monitor session	Configures SPAN or ERSPAN sessions.
show monitor session	Displays information about SPAN or ERSPAN sessions.

show running-config interface vethernet

To display the the currently running configuration for a virtual Ethernet interface, use the show running-config interface vethernet command.

show running-config interface vethernet veth-id [all | expand-port-profile]

Syntax Description

veth-id	Virtual Ethernet interface number. The range is from 1 to 1,048,575.
all	(Optional) Displays the full operating information including default settings.
expand-port-profile	(Optional) Displays the configuration information of port profiles.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the running configuration for a virtual Ethernet interface :

```
switch# show running-config interface vethernet 10
!Command: show running-config interface Vethernet10
!Time: Fri Jan  2 01:40:37 2009
version 5.1(3)N1(1)
interface Vethernet10
  inherit port-profile ppVEth
  untagged cos 3
  switchport access vlan 101
  bind interface Ethernet1/5 channel 10
switch#
```

This example shows how to display detailed information on the running configuration for a specified virtual Ethernet interface:

```
switch# show running-config interface vethernet 10 all
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.

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
	This command was introduced.

Examples

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

```
switch# show running-config callhome
!Command: show running-config callhome
!Time: Fri Jun 18 09:37:56 2010
version 5.0(2)N1(1)
callhome
  alert-group configuration user-def-cmd show ip routing
switch#
```

This example shows how to display the entire Call Home running configuration, including the default values:

```
switch# show running-config callhome all
!Command: show running-config callhome all
!Time: Fri Jun 18 09:38:03 2010
version 5.0(2)N1(1)
callhome
  switch-priority 7
  destination-profile CiscoTAC-1 transport-method email
  no destination-profile CiscoTAC-1 transport-method http
  destination-profile CiscoTAC-1 message-size 5000000
  destination-profile CiscoTAC-1 message-level 0
  destination-profile full_txt transport-method email
  no destination-profile full_txt transport-method http
  destination-profile full_txt message-size 2500000
  destination-profile full_txt message-level 0
  destination-profile short_txt transport-method email
  no destination-profile short_txt transport-method http
  destination-profile short_txt message-size 4000
  destination-profile short_txt message-level 0
  destination-profile CiscoTAC-1 alert-group cisco-tac
  destination-profile full_txt alert-group all
  destination-profile short_txt alert-group all
  alert-group configuration user-def-cmd show ip routing
  no enable
  duplicate-message throttle
```

```
  periodic-inventory notification
  periodic-inventory notification interval  7
  periodic-inventory notification timeofday 08:00
switch#
```

Related Commands

Command	Description
show callhome	Displays Call Home configuration information.

show run mmode

To display the currently running maintenance profile configuration on a switch, use the show run mmode command.

show run mmode [all]

Syntax Description

all	Displays the currently running maintenance profile configuration along with the defaults.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the currently running maintenance profile configuration on a switch:

```
switch(config)# show run mmode
!Command: show running-config mmode
!Time: Wed May 13 22:37:02 1970
version 7.3(0)N1(1)
configure maintenance profile normal-mode
  router isis 100
    no isolate
  router ospf 100
    no isolate
  router bgp 100
    no isolate
configure maintenance profile maintenance-mode
  router bgp 100
    isolate
  router ospf 100
    isolate
  router isis 100
    isolate
configure terminal
```

Related Commands

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

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

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
	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 ptp time-property

To display the PTP clock time properties, use the show ptp time-property command.

show ptp time-property

Syntax Description

There are no arguments or keywords for this command.

Command Default

None

Command History

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

Examples

This example shows how to display the PTP clock time properties:

```
switch(
config
)#
show ptp time-property
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clocks 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 and grandmaster clock.
show ptp port interface	Displays the status of the PTP port.

show ptp port interface

To display the status of the PTP port, use the show ptp port interface ethernet command.

show ptp port interface [ethernet slot/[QSFP-module/] port]

Syntax Description

ethernet	Specifies an Ethernet interface.
slot/[QSFP-module/]port	(Optional) Specifies the Ethernet interface and its slot number and port number. The slot number is from 1 to 255. The QSFP-module number is from 1 to 4. The port number is from 1 to 128. **Note** The QSFP-module number applies only to the QSFP+ Generic Expansion Module (GEM).

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to display the status of the PTP port on the switch:

```
switch(
config
)#
show ptp port interface ethernet 5/1
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clocks 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 interface	Displays the status of the PTP port.
show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
show ptp time-property	Displays the PTP clock time properties.

show ptp parent

To display the properties of the PTP parent and grandmaster clock, use the show ptp parent command.

show ptp parent

Syntax Description

There are no arguments or keywords for this command.

Command Default

None

Command History

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

Examples

This example shows how to display the properties of the PTP parent and grandmaster clock:

```
switch(
config
)#
show ptp parent
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp clocks 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 interface	Displays the status of the PTP port.
show ptp time-property	Displays the PTP clock time properties.

show ptp corrections

To display the last few PTP corrections, use the show ptp corrections command.

show ptp corrections

Syntax Description

There are no arguments or keywords for this command.

Command Default

None

Command History

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

Examples

This example shows how to display the most recent PTP corrections on the switch:

```
switch(
config
)#
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 clocks foreign-masters-record	Displays the state of foreign masters known to the PTP process.
show ptp port interface	Displays the status of the PTP port.
show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
show ptp time-property	Displays the PTP clock time properties.

show ptp clocks foreign-masters-record

To display the state of the foreign masters known to the PTP process, use the show ptp clocks foreign-masters-record command.

show ptp clocks foreign-masters-record [ethernet slot/[QSFP-module/] port]

Syntax Description

ethernet	Specifies an Ethernet interface.
slot/[QSFP-module/]port	(Optional) Specifies the Ethernet interface and its slot number and port number. The slot number is from 1 to 255. The QSFP-module number is from 1 to 4. The port number is from 1 to 128. **Note** The QSFP-module number applies only to the QSFP+ Generic Expansion Module (GEM).

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

For each foreign master, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster.

Examples

This example shows how to display the foreign masters known to the PTP process:

```
switch(
config
)#
show ptp foreign-masters-record
```

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 port interface	Displays the status of the PTP port.
show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
show ptp time-property	Displays the PTP clock time properties.

show ptp clock

To display the properties of the local PTP clock including clock identity, use the show ptp clock command.

show ptp clock

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to display the properties of the local clock:

```
switch(
config
)#
show ptp clock
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clocks 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 and grandmaster clock.
show ptp port interface	Displays the status of the PTP port.
show ptp time-property	Displays the PTP clock time properties.

show ptp brief

To display the PTP information, use the show ptp brief command.

show ptp brief

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to display the PTP status:

```
switch(
config
)#
show ptp brief
```

Related Commands

Command	Description
show ptp clock	Displays the properties of the local clock.
show ptp clocks 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 and grandmaster clock.
show ptp port interface	Displays the status of the PTP port.
show ptp time-property	Displays the PTP clock time properties.

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

Examples

This example shows how to display the NTP time-stamp status:

```
switch(
config
)#
show ntp timestamp-status
```

Related Commands

Command	Description
clear ntp statistics	Clears NTP statistics
ntp	Configures NTP peers and servers on the switch.

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 or IPv6 address. The IPv4 address format is dotted decimal, x.x.x.x. The IPv6 address format is hexadecimal A:B::C:D.
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
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the statistics for NTP:

```
switch(
config
)#
show ntp statistics local
```

Related Commands

Command	Description
clear ntp statistics	Clears NTP statistics

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

Examples

This example shows how to display the peer status for NTP:

```
switch(
config
)#
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
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display information about NTP peers:

```
switch(
config
)#
show ntp peers
```

Related Commands

Command	Description
show ntp peer-status	Displays status information about NTP peers.

show ntp authentication-status

To display the status of the Network Time Protocol (NTP) authentication, use the show ntp authentication-status command.

show ntp authentication-status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

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

Examples

This example shows how to display the authentication status for NTP:

```
switch(
config
)#
show ntp authentication-status
```

Related Commands

Command	Description
[no] ntp authenticate	Displays information about NTP peers.

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] | status]

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.
status	(Optional) Displays the operational state of all sessions. **Note** This keyword applies only to SPAN sessions.

Command Default

None

Command Modes

EXEC mode

Command History

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

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 brief information about a SPAN session:

```
switch# show monitor session range 1 brief
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 VSANs      :
destination ports : Eth1/21
Legend: f = forwarding enabled, l = learning enabled
switch#
```

This example shows how to display the information about an ERSPAN session:

```
switch# show monitor session 1
session 1
---------------
description       : ERSPAN Source configuration
type              : erspan-source
state             : down (No valid global IP Address)
flow-id           : 1
vrf-name          : default
destination-ip    : 192.0.2.1
ip-ttl            : 255
ip-dscp            : 0
origin-ip         : origin-ip not specified
source intf       :
    rx            : Eth1/5
    tx            : Eth1/5
    both          : Eth1/5
source VLANs      :
    rx            : 5
switch#
```

Related Commands

Command	Description
monitor session	Creates a new Switched Port Analyzer (SPAN) session configuration.
show running-config monitor	Displays the running configuration information about SPAN sessions.

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

Examples

This example shows how to display the logging status:

```
switch# show logging status

Fabric Distribute     : Enabled
Session State         : IDLE
switch#
```

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 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
5.2(1)N1(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 level	Enables logging messages from a defined facility.

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
5.2(1)N1(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 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
5.2(1)N1(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
switch#
```

Related Commands

Command	Description
logging abort	Cancels the pending changes to the syslog server configuration.

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

Examples

This example shows how to display the pending changes to the syslog server configuration:

```
switch# show logging pending
switch#
```

Related Commands

Command	Description
logging abort	Cancels the pending changes to the syslog server configuration.

show logging onboard

To display the onboard logging information based on the error type, use the show logging onboard command.

show logging onboard boot-uptime | device-version | endtime | environmental-history | exception-log | kernel-trace | obfl-history | obfl-logs | stack-trace | starttime | status [>file | type]

Syntax Description

boot-uptime	Displays the onboard failure logging (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.
> 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
5.2(1)N1(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] —Begin 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

----------------------------
OBFL Data for
    Module:  0
----------------------------
Sun Dec 16 16:03:39 2012:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Sun Dec 16 16:03:39 2012
Module Number......:  1
Serial Number......:  FOC16191MQ1
Bios Version.......:
Firmware Version...:
Sun Dec 16 16:44:08 2012:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Sun Dec 16 16:44:07 2012
Module Number......:  0
Serial Number......:  FOC16192WJZ
Bios Version.......:    v1.2.0(06/09/12)
Firmware Version...:  6.0(2)N1(1) [build 6.0(2)N1(0.365.5P)]
--More--
```

Table 1 describes the significant fields shown in the display.

Table 2: show logging onboard boot-uptime Command Output

Field	Description
Boot Time	Time boot occurred.

Field	Description
Slot Number	Slot number.
Serial Number	Serial number of the module.
Bios Version	Primary binary input and output system (BIOS) version.
Firmware Version	Firmware version.

This example shows how to display the OBFL logging device information:

```
switch# show logging onboard device-version

----------------------------
OBFL Data for
    Module:  1
----------------------------
Device Version Record
-------------------------------------------------------------------------
Timestamp                 Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Sun Nov  3 07:07:00 2008  GATOS                 2        2        0
Sun Nov  3 07:07:00 2008  GATOS                 3        2        0
Sun Nov  3 07:07:00 2008  GATOS                 4        2        0
Sun Nov  3 07:07:00 2008  GATOS                 5        2        0
Sun Nov  3 07:07:00 2008  GATOS                 6        2        0
Sun Nov  3 07:07:00 2008  GATOS                 7        2        0
Sun Nov  3 07:07:00 2008  GATOS                 8        2        0
Sun Nov  3 07:07:00 2008  GATOS                 9        2        0
Sun Nov  3 07:07:00 2008  GATOS                10        2        0
Sun Nov  3 07:07:00 2008  GATOS                11        2        0
Sun Nov  3 07:07:00 2008  GATOS                12        2        0
Sun Nov  3 07:07:00 2008  GATOS                13        2        0
Mon Nov  4 00:15:08 2008  ALTOS                 0        2        0
Mon Nov  4 00:15:08 2008  GATOS                 0        2        0
Mon Nov  4 00:15:08 2008  GATOS                 1        2        0
Mon Nov  4 00:15:08 2008  GATOS                 2        2        0
```

Table 2 describes the significant fields shown in the display.

Table 3: show logging onboard device-version Command Output

Field	Description
Timestamp	Day, date, and time.
Device Name	Device name.
Instance Num	Number of instances.
Hardware Version	Hardware device version.
Software Version	Software 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

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 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
5.2(1)N1(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 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
5.2(1)N1(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 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
5.2(1)N1(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 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
5.2(1)N1(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 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. The facilities are listed in Table 1-1 of Appendix 1, "System Message Logging Facilities."

Command Default

None

Command Modes

EXEC mode

Command History

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

Examples

This example shows how to display the EtherChannel logging severity level configuration:

```
switch# show logging level port-channel
```

This example shows how to display the Flex Links logging severity level configuration:

```
switch# show logging level flexlink

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
Flexlink                2                       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 FCoE NPV logging severity level configuration:

```
switch# show logging level fcoe_mgr

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcoe_mgr                2                       3
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

This example shows how to display the Power over Ethernet (PoE) logging severity level configuration:

```
switch# show logging level poed
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
```

```
poe                     5                       5
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 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
5.2(1)N1(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 level	Enables logging messages from a defined facility.

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

Examples

This example shows how to display the logging configuration:

```
switch# show logging info
```

Related Commands

Command	Description
logging level	Enables logging messages from a defined facility.

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
5.2(1)N1(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 ip dns source-interface

To display the source interfaces configured for Domain Name Server (DNS) domain lookup, use the show ip dns source-interface command.

show ip dns source-interface [vrf vrf-name | all | default | management]

Syntax Description

vrf	(Optional) Displays information about the virtual routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name. The name is case sensitive and can be a maximum of 32 characters.
all	(Optional) Displays all VRF instances.
default	(Optional) Displays the default VRF information.
management	(Optional) Displays the management VRF information.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the source interfaces configured for DNS domain lookup:

```
switch# show ip dns source-interface
VRF Name                                Interface
default                                 Ethernet1/5
switch#
```

Related Commands

Command	Description
ip domain-lookup	Enables the DNS lookup feature.
ip dns source-interface	Configures interfaces for DNS domain lookup.

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

Examples

This example shows how to display the IP addresses of the DNS servers that are used to resolve host names:

```
switch# show hosts
DNS lookup enabled
Default domain for vrf:default is mysite.com
Name/address lookup uses domain service
Name servers are 255.255.255.255
Vrf                 Use-vrf             Token           Config
default             management          domain          mysite.com
default             management          add. domain(s)  mysite2.com
Host                   Address
switch#
```

Related Commands

Command	Description
ip domain-list	Defines a list of domains.
ip domain lookup	Enables DNS-based host name-to-address translation.
ip domain-name	Configures a name server.

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
5.2(1)N1(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

Current bootup diagnostic level: complete
Module 1: 48X10GE/Supervisor  SerialNo : JAF1339ANGH
  Overall Diagnostic Result for Module 1 : PASS
  Diagnostic level at card bootup: complete
  Test results: (. = Pass, F = Fail, I = Incomplete,
                 U = Untested, A = Abort)
     1) TestUSBFlash ----------------------> .
     2) TestSPROM -------------------------> .
     3) TestPCIe --------------------------> .
     4) TestLED ---------------------------> .
     5) TestOBFL --------------------------> .
     6) TestNVRAM -------------------------> .
     7) TestPowerSupply -------------------> F
     8) TestTemperatureSensor -------------> .
     9) TestFan ---------------------------> .
    10) TestVoltage ----------------------> .
    11) TestGPIO -------------------------> .
    12) TestInbandPort -------------------> .
    13) TestManagementPort ---------------> .
    14) TestMemory -----------------------> .
    15) TestFabricEngine :
   Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
   Port ---------------------------------------------------------------------
          .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
   Eth   25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
   Port ---------------------------------------------------------------------
          .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
    16) TestFabricPort :
   Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
```

```
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
    Eth   25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
     17) TestForwardingEngine :
    Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
    Eth   25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
     18) TestForwardingEnginePort :
    Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
    Eth   25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
     19) TestFrontPort :
    Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
    Eth   25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
    Port --------------------------------------------------------------------
           .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
switch#
```

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

Examples

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

```
switch# show diagnostic bootup level

        Current bootup diagnostic level: complete
switch#
```

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 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
	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 system soft-reload status

To display the status of the soft reload, use the show system soft-reload status command.

show system soft-reload status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the status of the soft reload:

```
switch# show system soft-reload status
Soft-reload is disabled
```

Related Commands

Command	Description
soft-reload	Performs a manual soft reload of the switch.
system soft-reload enable	Enables the switch to perform a soft reload after a process crash.

V Commands

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

Examples

This example shows how to verify a session:

```
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 both the source and destination, use the vrf command. To revert to the defaults, 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

network-admin network-operator

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to 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 or SPAN session for analyzing traffic between ports.
show monitor session	Displays information about the Ethernet switched port analyzer (SPAN) or ERSPAN monitor session.

System Message Logging Facilities

System Message Logging Facilities

This appendix contains the system message logging information. Table 1-1 lists the facilities that you can use in system message logging configuration.

Table 4: System Message Logging Facilities

Facility	Description
aaa	Sets level for aaa syslog messages.
aclmgr	Sets level for aclmgr syslog messages.
adjmgr	Sets syslog filter level for Adjacency Manager.
afm	Sets level for afm syslog messages.
all	Sets level for all facilities.
altos	Altos syslog level.
arp	Sets syslog filter level for ARP.
ascii-cfg	Sets the logging level for ascii-cfg.
auth	Sets level for Authorization System.
authpriv	Sets level for Authorization (Private) system.
backup	Sets level for switchport backup syslog messages.
bootvar	Sets level for bootvar.
callhome	Callhome syslog level.
capability	Sets syslog level for mig utils daemon.
cdp	Sets logging level for CDP.
cert-enroll	Cert-enroll syslog level.
cfs	Sets logging level for CFS.
clis	Sets syslog filter level for CLIS.
core	Core daemon syslog level.
cron	Sets level for Cron/at facility.
daemon	Sets level for System daemons.
dcbx	Sets level for dcx syslog messages.
device-alias	Sets syslog level for Device Alias Distribution Service.

Facility	Description
dhcp_snoop	Sets the level for DHCP snooping syslog messages.
dstats	Delta statistics syslog level.
epp	Sets level for EPP syslog messages.
ethpc	Sets level for ethpc syslog messages.
ethpm	Sets level for Ethernet Port Manager (ethpm) syslog messages.
evmc	Sets level for evmc syslog messages.
fabric_start_cfg_mgr	Sets the syslog filter level for FabricPath configuration manager.
fc2d	Sets level for fc2d syslog messages.
fcdomain	Sets level for fcdomain syslog messages.
fcns	Sets syslog filter level for name server.
fcoe_mgr	Sets the level for Fibre Channel over Ethernet (FCoE) manager syslog messages.
fcpc	Sets level for fcpc syslog messages.
fcs	Sets syslog filter level for FCS.
fdmi	Sets logging level for fdmi.
feature-mgr	Feature manager syslog level.
fex	Sets the level for Cisco Nexus 2000 Series Fabric Extender syslog messages.
flexlink	Sets level for switchport backup syslog messages.
flogi	Configure level for flogi syslog messages.
fs-daemon	FS daemon syslog level.
fspf	FSPF syslog level.
ftp	Sets level for File Transfer System.
fwm	Sets level for fwm syslog messages.
gatos	Gatos syslog level.
im	Sets level for im syslog messages.
interface-vlan	Sets level for interface VLAN syslog messages.
ip	Sets level for IP syslog messages.
ipconf	Sets level for ipconf syslog messages.
ipqos	Sets level for ipqosmgr syslog messages.

Facility	Description
kernel	Sets level for kernel.
l3vm	Sets syslog filter level for L3VM.
lacp	Sets level for LACP syslog messages.
license	Licensing syslog level. **Note** This facility was deprecated and replaced with the licmgr facility in Cisco NX-OS 5.0(2)N1(1). For backwards compatibility, it will be maintained for a number of releases.
licmgr	Licensing syslog level.
lldp	Sets level for LLDP syslog messages.
local0	Sets level for Local use daemons.
local1	Sets level for Local use daemons.
local2	Sets level for Local use daemons.
local3	Sets level for Local use daemons.
local4	Sets level for Local use daemons.
local5	Sets level for Local use daemons.
local6	Sets level for Local use daemons.
local7	Sets level for Local use daemons.
lpr	Sets level for Line Printer System.
m2rib	Sets level for Multicast Routing Information Base (MRIB) logging messages.
mail	Sets level for Mail system.
mfdm	Sets level for multicast Forwarding Information Base (FIB) distribution (MFDM) syslog messages.
mfwd	Sets level for multicast forwarding system messages.
monitor	Sets level for ethernet Switched Port Analyzer (SPAN) syslog messages.
news	Sets level for USENET news.
nohms	Sets level for nohms syslog messages.
nqosm	Sets level for nqosm syslog messages.
ntp	Sets syslog filter level for NTP.
pfm	Sets level for pfm syslog messages.

Facility	Description
pktmgr	Sets syslog filter level for Packet Manager.
plugin	Sets level for plugin syslog messages.
port	Sets level for port syslog messages.
port-channel	Sets level for EtherChannel syslog messages.
port-profile	Sets level for port profile syslog messages.
port-resources	Sets level for prm syslog messages.
provision	Sets level for provision syslog messages.
qd	Sets level for qd syslog messages.
radius	RADIUS syslog level.
rdl	Sets logging level for RDL.
res_mgr	Set slevel for res_mgr syslog messages.
rib	Sets level for rib.
rlir	Sets level for RLIR.
routing	Sets level for routing information.
rscn	Sets level for RSCN.
san-port-channel	Sets level for san-port-channel syslog messages.
scsi-target	SCSI target daemon syslog level.
security	Security syslog level.
session	Sets level for session-manager syslog messages. **Note** This facility was deprecated and replaced with the session-mgr facility in Cisco NX-OS 5.0(2)N1(1). For backward compatibility, it will be maintained for a number of releases.
session-mgr	Sets level for session-manager syslog messages.
smm	Sets logging level for Shared Memory Manager.
snmpd	Sets level for SNMP syslog messages.
sifmgr	Sets level for sifmgr syslog messages.
spanning-tree	Sets level for stp syslog messages.
stp	Sets level for stp syslog messages.
syslog	Sets level for Internal Syslog Messages.

Facility	Description
sysmgr	System Manager syslog level.
tacacs	TACACS+ syslog level.
track	Sets level for object tracking messages.
tcpudp	Sets syslog filter level for TCPUDP.
track	Sets level for track syslog messages.
udld	Sets level for UDLD syslog messages.
ufdm	Sets level for unicast Forwarding Information Base (FIB) distribution (UFDM) syslog messages.
urib	Sets syslog filter level for Unicast Routing Information Base (URIB).
user	Sets level for User Process.
uucp	Sets level for Unix-to-Unix copy system.
vlan_mgr	Sets level for VLAN syslog messages.
vmm	Sets level for vmm syslog messages.
vpc	Sets level for vPC syslog messages.
vsan	VSAN syslog level.
vshd	Sets logging level for vshd.
vtp	Sets level for interface vlan syslog messages.
wwnm	Sets WWN Manager syslog level.
xml	XML agent syslog level.
zone	Sets syslog filter level for zone server.
zschk	Sets level for zschk syslog messages.