Send comments to nx5000-docfeedback@cisco.com

Cisco Nexus 5000 Series NX-OS Command Reference

Cisco NX-OS Releases 4.1(3)N1(1), 4.1(3)N1(1a), 4.1(3)N2(1), 4.2(1)N1(1), 4.2(1)N2(1)

November 2010

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

Text Part Number: OL-22746-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Nexus 5000 Series NX-OS Command Reference
© 2010 Cisco Systems, Inc. All rights reserved.

Send comments to nx5000-docfeedback@cisco.com

CONTENTS

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 5000 Series NX-OS Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

Audience

This publication is for experienced users who configure and maintain Cisco NX-OS devices.

Organization

This reference is organized as follows:

Chapter	Title	Description
Chapter 1	Basic System Commands	Describes the basic Cisco NX-OS system commands.
Chapter 2	Ethernet Commands	Describes the Cisco NX-OS Ethernet commands.
Chapter 3	Ethernet Show Commands	Describes the Cisco NX-OS Ethernet show commands.
Chapter 4	Fabric Extender Commands	Describes the Cisco NX-OS Fabric Extender commands.
Chapter 5	Quality of Service Commands	Describes the Cisco NX-OS quality of service commands.
Chapter 6	Security Commands	Describes the Cisco NX-OS security commands.

Send comments to nx5000-docfeedback@cisco.com

Chapter	Title	Description
Chapter 8	Fibre Channel Commands	Describes the Cisco NX-OS Fibre Channel, virtual Fibre Channel, and Fibre Channel over Ethernet (FCoE) commands.
Chapter 9	Fibre Channel Show Commands	Describes the Cisco NX-OS Fibre Channel and Fibre Channel over Ethernet (FCoE) show commands.
Chapter 10	vPC Commands	Describes the Cisco NX-OS virtual port channel (vPC) commands.
Chapter 7	System Management Commands	Describes the Cisco NX-OS system management commands.

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information 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.

Send comments to nx5000-docfeedback@cisco.com

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 and Cisco Nexus 2000 Series Fabric Extender is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

The following are related Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender documents:

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1)

Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide

Cisco Nexus 5000 Series NX-OS Fundamentals Configuration Guide

Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

Cisco Nexus 5000 Series Switch CLI Software Configuration Guide

Cisco Nexus 5000 Series Hardware Installation Guide

Cisco NX-OS System Messages Reference

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Cisco Nexus 2000 Series Fabric Extender Hardware Installation Guide

Cisco Nexus 5000 Series Fabric Manager Software Configuration Guide

Obtaining Documentation and Submitting a Service Request

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

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

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

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 1

Basic System Commands

This chapter describes the basic Cisco NX-OS system commands available on Cisco Nexus 5000 Series switches. These commands allow you to navigate and control the switch.

Send comments to nx5000-docfeedback@cisco.com

banner motd

To configure the message-of-the-day (MOTD) banner that displays when the user logs in to a Cisco Nexus 5000 Series switch, use the **banner motd** command. To revert to the default, use the **no** form of this command.

banner motd *delimiter message delimiter*

no banner motd

Syntax Description

delimiter	Delimiter character that indicates the start and end of the message and is not a character that you use in the message. Do not use **"** or **%** as a delimiting character. White space characters will not work.
message	Message text. The text is alphanumeric, case sensitive, and can contain special characters. It cannot contain the delimiter character you have chosen. The text has a maximum length of 80 characters and a maximum of 40 lines.

Command Default

"Nexus 5000 Switch" is the default MOTD string.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To create a multiple-line MOTD banner, press **Enter** before typing the delimiting character to start a new line. You can enter up to 40 lines of text.

Examples

This example shows how to configure a single-line MOTD banner:

```
switch(config)# banner motd #Unauthorized access to this device is prohibited!#
```

This example shows how to configure a multiple-line MOTD banner:

```
switch(config)# banner motd #Welcome Authorized Users Unauthorized access prohibited!#
```

This example shows how to revert to the default MOTD banner:

```
switch(config)# no banner motd
```

Related Commands

Command	Description
show banner motd	Displays the MOTD banner.

Send comments to nx5000-docfeedback@cisco.com

boot

To configure the boot variable for the Cisco Nexus 5000 Series kickstart or system software image, use the **boot** command. To clear the boot variable, use the **no** form of this command.

boot {**kickstart** | **system**} [**bootflash:**] [*//server/*] [*directory*] *filename*

no boot {**kickstart** | **system**}

Syntax Description

kickstart	Configures the kickstart image.
system	Configures the system image.
bootflash:	(Optional) Specifies the name of the bootflash file system.
//server/	(Optional) Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the kickstart or system image file. The filename is case sensitive.

Note There can be no spaces in the *bootflash://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software uses the boot variable for loading images when booting up. You must copy the correct image to the switch before you reload.

Examples

This example shows how to configure the system boot variable:

```
switch(config)# boot system bootflash:n5000.bin
```

This example shows how to configure the kickstart boot variable:

```
switch(config)# boot kickstart bootflash:n5000-kickstart.bin
```

This example shows how to clear the system boot variable:

```
switch(config)# no boot system
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to clear the kickstart boot variable:

```
switch(config)# no boot kickstart
```

Related Commands

Command	Description
copy	Copies files.
show boot	Displays boot variable configuration information.

Send comments to nx5000-docfeedback@cisco.com

cd

To change the current working directory in the device file system, use the **cd** command.

cd [*filesystem***:**] [*//server/*] *directory*

Syntax Description

*filesystem***:**	(Optional) Name of the file system. Valid values are **bootflash** or **volatile**.
//server/	(Optional) Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	Name of the destination directory. The directory name is case sensitive.

Note There can be no spaces in the *filesystem://server/directory* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default None

Command Modes EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines Use the **pwd** command to verify the current working directory.

Examples This example shows how to change the current working directory on the current file system:

```
switch# cd my-scripts
```

This example shows how to change the current working directory to another file system:

```
switch# cd volatile:
```

Related Commands

Command	Description
pwd	Displays the current working directory name.

Send comments to nx5000-docfeedback@cisco.com

clear cli history

To clear the command history, use the **clear cli history** command.

clear cli history

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **show cli history** command to display the history of the commands that you entered at the command-line interface (CLI).

Examples

This example shows how to clear the command history:

```
switch# clear cli history
```

Related Commands

Command	Description
show cli history	Displays the command history.

Send comments to nx5000-docfeedback@cisco.com

clear cores

To clear the core files, use the **clear cores** command.

clear cores

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **show system cores** command to display information about the core files.

Examples

This example shows how to clear the core file:

```
switch# clear cores
```

Related Commands

Command	Description
show system cores	Displays the core filename.
system cores	Configures the core filename.

Send comments to nx5000-docfeedback@cisco.com

clear debug-logfile

To clear the contents of the debug log file, use the **clear debug-logfile** command.

clear debug-logfile *filename*

Syntax Description

filename	Name of the debug log file to clear.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the debug log file:

```
switch# clear debug-logfile syslogd_debugs
```

Related Commands

Command	Description
debug logfile	Configures a debug log file.
debug logging	Enables debug logging.
show debug logfile	Displays the contents of the debug log file.

Send comments to nx5000-docfeedback@cisco.com

clear install failure-reason

To clear the reason for software installation failures, use the **clear install failure-reason** command.

clear install failure-reason

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the reason for software installation failures:

```
switch# clear install failure-reason
```

Related Commands

Command	Description
show install all	Displays status information for the software installation.

Send comments to nx5000-docfeedback@cisco.com

clear license

To uninstall a license, use the **clear license** command.

clear license *filename*

Syntax Description		
	filename	Name of the license file to be uninstalled.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to clear a specific license:

```
switch# clear license fm.lic
```

Related Commands	Command	Description
	show license	Displays license information.

Send comments to nx5000-docfeedback@cisco.com

clear user

To log out a particular user, use the **clear user** command.

clear user *username*

Syntax Description		
	username	Name of the user to be logged out.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to log out a specific user:

```
switch# clear user admin
```

Related Commands	Command	Description
	show users	Displays the users currently logged on the switch.

Send comments to nx5000-docfeedback@cisco.com

cli var name

To define a command-line interface (CLI) variable for a terminal session, use the **cli var name** command. To remove the CLI variable, use the **no** form of this command.

cli var name *variable-name variable-text*

no cli var name *variable-name*

Syntax Description

variable-name	Name of the variable. The name is alphanumeric, case sensitive, and has a maximum of 31 characters.
variable-text	Variable text. The text is alphanumeric, can contain spaces, and has a maximum of 200 characters.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can reference a CLI variable using the following syntax:

`$(variable-name)`

Instances where you can use variables include the following:

- Command scripts
- Filenames

You cannot reference a variable in the definition of another variable.

The Cisco NX-OS software provides a predefined variable, TIMESTAMP, that you can use to insert the time of day. You cannot change or remove the TIMESTAMP CLI variable.

You cannot change the definition of a CLI variable. You must remove the variable and then create it again with the new definition.

Examples

This example shows how to define a CLI variable:

```
switch# cli var name testvar interface ethernet 1/3
```

This example shows how to reference a CLI variable:

```
switch# show $(testvar)
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to reference the TIMESTAMP variable:

```
switch# copy running-config > bootflash:run-config-$(TIMESTAMP).cnfg
```

This example shows how to remove a CLI variable:

```
switch# cli no var name testvar
```

Related Commands

Command	Description
run-script	Runs command scripts.
show cli variables	Displays the CLI variables.

Send comments to nx5000-docfeedback@cisco.com

clock set

To manually set the clock on a Cisco Nexus 5000 Series switch, use the **clock set** command.

clock set *time day month year*

Syntax Description

time	Time of day. The format is *HH*:*MM*:*SS*.
day	Day of the month. The range is from 1 to 31.
month	Month of the year. The values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
year	Year. The range is from 2000 to 2030.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command when you cannot synchronize the switch with an outside clock source, such as an NTP server.

Examples

This example shows how to manually configure the clock:

```
switch# clock set 12:00:00 04 July 2008
```

Related Commands

Command	Description
show clock	Displays the clock time.

Send comments to nx5000-docfeedback@cisco.com

clock summer-time

To configure the summer-time (daylight saving time) offset, use the **clock summer-time** command. To revert to the default, use the **no** form of this command.

clock summer-time *zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes*

no clock summer-time

Syntax Description

zone-name	Time zone string. The time zone string is a three-character string.
start-week	Week of the month to start the summer-time offset. The range is from 1 to 5.
start-day	Day of the month to start the summer-time offset. Valid values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
start-month	Month to start the summer-time offset. Valid values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
start-time	Time to start the summer-time offset. The format is *HH*:*MM*.
end-week	Week of the month to end the summer-time offset. The range is from 1 to 5.
end-day	Day of the month to end the summer-time offset. Valid values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
end-month	Month to end the summer-time offset. Valid values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
end-time	Time to end the summer-time offset. The format is *HH*:*MM*.
offset-minutes	Number of minutes to offset the clock. The range is from 1 to 1440.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure the offset for summer-time or daylight saving time:

```
switch(config)# clock summer-time PDT 1 Sunday March 02:00 5 Sunday November 02:00 60
```

This example shows how to revert to the default offset for summer-time:

```
switch(config)# no clock summer-time
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show clock	Displays the clock summer-time offset configuration.

Send comments to nx5000-docfeedback@cisco.com

clock timezone

To configure the time zone offset from Coordinated Universal Time (UTC), use the **clock timezone** command. To revert to the default, use the **no** form of this command.

clock timezone *zone-name offset-hours offset-minutes*

no clock timezone

Syntax Description

zone-name	Zone name. The name is a 3-character string for the time zone acronym (for example, PST or EST).
offset-hours	Number of hours offset from UTC. The range is from –23 to 23.
offset-minutes	Number of minutes offset from UTC. The range is from 0 to 59.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to offset the device clock from UTC.

Examples

This example shows how to configure the time zone offset from UTC:

```
switch(config)# clock timezone PST -8 0
```

This example shows how to revert the time zone offset to the default:

```
switch# no clock timezone
```

Related Commands

Command	Description
show clock	Displays the clock time.

Send comments to nx5000-docfeedback@cisco.com

configure session

To create or modify a configuration session, use the **configure session** command.

configure session *name*

Syntax Description

name	Name of the session. The name is a case-sensitive alphanumeric string up to 63 characters.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Examples

This example shows how to create a configuration session:

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

Related Commands

Command	Description
show configuration session	Displays information about the configuration sessions.

Send comments to nx5000-docfeedback@cisco.com

configure terminal

To enter configuration mode, use the **configure terminal** command.

configure terminal

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to enter configuration mode. Commands in this mode are written to the running configuration file as soon as you enter them (using the **Enter** key/**Carriage Return**).

After you enter the **configure terminal** command, the system prompt changes from switch# to switch(config)#, indicating that the router is in configuration mode. To leave configuration mode and return to EXEC mode, type **end** or press **Ctrl-Z**.

To view the changes to the configuration that you have made, use the **show running-config** command.

Examples

This example shows how to enter configuration mode:

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

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration as the startup configuration file.
end	Ends your configuration session by exiting to EXEC mode.
exit (global)	Exits from the current configuration mode to the next highest configuration mode.
show running-config	Displays the current running configuration.

Send comments to nx5000-docfeedback@cisco.com

copy

To copy any file from a source to a destination, use the **copy** command.

copy *source-url destination-url*

Syntax Description

source-url	Location URL (or variable) of the source file or directory to be copied. The source can be either local or remote, depending upon whether the file is being downloaded or uploaded. For more information, see the “Usage Guidelines” section.
destination-url	Destination URL (or variable) of the copied file or directory. The destination can be either local or remote, depending upon whether the file is being downloaded or uploaded. For more information, see the “Usage Guidelines” section.

Command Default

The default name for the destination file is the source filename.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **copy** command allows you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file is specified using a Cisco NX-OS file system URL, which allows you to specify a local or remote file location. The file system being used (such as a local memory source or a remote server) determines the syntax used in the command.

You can enter on the command line all necessary source- and destination-URL information and the username to use, or you can enter the **copy** command and have the CLI prompt you for any missing information.

The entire copying process may take several minutes, depending on the network conditions and the size of the file, and differs from protocol to protocol and from network to network.

The colon character (**:**) is required after the file system URL prefix keywords (such as **bootflash**).

In the URL syntax for **ftp:**, **scp:**, **sftp:**, and **tftp:**, the server is either an IPv4 address or a hostname.

Format of Source and Destination URL

The format of the source and destination URLs varies according to the file or directory location. You can enter either a command-line interface (CLI) variable for a directory or a filename that follows the Cisco NX-OS file system syntax (*filesystem*:[/*directory*][/*filename*]).

The following tables list URL prefix keywords by the file system type. If you do not specify a URL prefix keyword, the router looks for a file in the current directory.

Send comments to nx5000-docfeedback@cisco.com

Table 1-1 lists URL prefix keywords for local writable storage file systems. Table 1-2 lists the URL prefix keywords for remote file systems. Table 1-3 lists the URL prefix keywords for nonwritable file systems.

Table 1-1 URL Prefix Keywords for Local Writable Storage File Systems

Keyword	Source or Destination
bootflash:[*//server/*]	Source or destination URL for boot flash memory. The *server* argument value is **module-1**, **sup-1**, **sup-active**, or **sup-local**.
volatile:[*//server/*]	Source or destination URL of the default internal file system. Any files or directories stored in this file system will be erased when the switch reboots. The *server* argument value is **module-1**, **sup-1**, **sup-active**, or **sup-local**.

Table 1-2 URL Prefix Keywords for Remote File Systems

Keyword	Source or Destination
ftp:	Source or destination URL for a FTP network server. The syntax for this alias is as follows: **ftp:**[*//server*][*/path*]*/filename*
scp:	Source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). The syntax for this alias is as follows: **scp:**[*//*[*username***@**]*server*][*/path*]*/filename*
sftp:	Source or destination URL for an SSH FTP (SFTP) network server. The syntax for this alias is as follows: **sftp:**[*//*[*username***@**]*server*][*/path*]*/filename*
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is as follows: **tftp:**[*//server*[**:***port*]][*/path*]*/filename*

Table 1-3 URL Prefix Keywords for Special File Systems

Keyword	Source or Destination
core:	Local memory for core files. You can copy core files from the core file system.
debug:	Local memory for debug files. You can copy core files from the debug file system.
log:	Local memory for log files. You can copy log files from the log file system.
modflash:	External memory for mod files. You can copy mod files from modflash file system.
system:	Local system memory. You can copy the running configuration to or from the system file system. The system file system is optional when referencing the running-config file in a command.
volatile:	Local volatile memory. You can copy files to or from the volatile file system. All files in the volatile memory are lost when the physical device reloads.

Send comments to nx5000-docfeedback@cisco.com

This section contains usage guidelines for the following topics:

Copying Files from a Server to Bootflash Memory

Use the **copy** *source-url* **bootflash:** command (for example, **copy tftp:***source-url* **bootflash:**) to copy an image from a server to the local bootflash memory.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy** {**ftp:** | **scp:** | **sftp:** | **tftp:**}*source-url* **running-config** command to download a configuration file from a network server to the running configuration of the device. The configuration is added to the running configuration as if the commands were typed in the CLI. The resulting configuration file is a combination of the previous running configuration and the downloaded configuration file. The downloaded configuration file has precedence over the previous running configuration.

You can copy either a host configuration file or a network configuration file. Accept the default value of *host* to copy and load a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and load a network configuration file that contains commands that apply to all network servers on a network.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy** {**ftp:** | **scp:** | **sftp:** | **tftp:**}*source-url* **startup-config** command to copy a configuration file from a network server to the router startup configuration. These commands replace the startup configuration file with the copied configuration file.

Copying the Running or Startup Configuration on a Server

Use the **copy running-config** {**ftp:** | **scp:** | **sftp:** | **tftp:**}*destination-url* command to copy the current configuration file to a network server that uses FTP, scp, SFTP, or TFTP. Use the **copy startup-config** {**ftp:** | **scp:** | **stfp:** | **tftp:**}*destination-url* command to copy the startup configuration file to a network server.

You can use the copied configuration file copy as a backup.

Examples

This example shows how to copy a file within the same directory:

```
switch# copy file1 file2
```

This example shows how to copy a file to another directory:

```
switch# copy file1 my-scripts/file2
```

This example shows how to copy a file to another file system:

```
switch# copy file1 bootflash:
```

This example shows how to copy a file to another supervisor module:

```
switch# copy file1 bootflash://sup-1/file1.bak
```

This example shows how to copy a file from a remote server:

Send comments to nx5000-docfeedback@cisco.com

```
switch# copy scp://192.168.1.1/image-file.bin bootflash:image-file.bin
```

Related Commands

Command	Description
cd	Changes the current working directory.
delete	Delete a file or directory.
dir	Displays the directory contents.
move	Moves a file.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

copy running-config startup-config

To save the running configuration to the startup configuration file so that all current configuration details are available after a reboot, use the **copy running-config startup-config** command.

copy running-config startup-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To view the changes to the configuration that you have made, use the **show startup-config** command.

Note Once you enter the **copy running-config startup-config** command, the running and the startup copies of the configuration are identical.

Examples

This example shows how to save the running configuration to the startup configuration:

```
switch# copy running-config startup-config
```

Related Commands

Command	Description
show running-config	Displays the currently running configuration.
show startup-config	Displays the startup configuration file.

Send comments to nx5000-docfeedback@cisco.com

databits

To configure the number of data bits in a character for the terminal port, use the **databits** command. To revert to the default, use the **no** form of this command.

databits *bits*

no databits *bits*

Syntax Description

bits	Number of data bits in a character. The range is from 5 to 8.

Command Default

8 bits

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the number of data bits for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# databits 7
```

This example shows how to revert to the default number of data bits for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no databits 7
```

Related Commands

Command	Description
show line	Displays information about the console port configuration.

Send comments to nx5000-docfeedback@cisco.com

debug logfile

To direct the output of the **debug** commands to a specified file, use the **debug logfile** command. To revert to the default, use the **no** form of this command.

debug logfile *filename* [**size** *bytes*]

no debug logfile *filename* [**size** *bytes*]

Syntax Description

filename	Name of the file for **debug** command output. The filename is alphanumeric, case sensitive, and has a maximum of 64 characters.
size *bytes*	(Optional) Specifies the size of the log file in bytes. The range is from 4096 to 4194304.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software creates the logfile in the log: file system root directory. Use the **dir log:** command to display the log files.

Examples

This example shows how to specify a debug log file:

```
switch# debug logfile debug_log
```

This example shows how to revert to the default debug log file:

```
switch# no debug logfile debug_log
```

Related Commands

Command	Description
dir	Displays the contents of a directory.
show debug logfile	Displays the debug logfile contents.

Send comments to nx5000-docfeedback@cisco.com

debug logging

To enable **debug** command output logging, use the **debug logging** command. To disable debug logging, use the **no** form of this command.

debug logging

no debug logging

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable the output logging for the **debug** command:

```
switch# debug logging
```

This example shows how to disable the output logging for the **debug** command:

```
switch# no debug logging
```

Related Commands

Command	Description
debug logfile	Configures the log file for the **debug** command output.

Send comments to nx5000-docfeedback@cisco.com

delete

To delete a file or directory, use the **delete** command.

delete [*filesystem***:**] [*//server/*] [*directory*] *filename*

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **debug**, **log**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the file to delete. The filename is case sensitive.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **dir** command to locate the file you that want to delete.

The **delete** command will delete a directory and its contents. Exercise caution when using this command to delete directories.

Examples

This example shows how to delete a file:

```
switch# delete bootflash:old_config.cfg
```

This example shows how to delete a directory:

```
switch# delete my_dir
This is a directory.  Do you want to continue (y/n)?  [y] y
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
dir	Displays the contents of a directory.
save	Saves the configuration session to a file.

Send comments to nx5000-docfeedback@cisco.com

dir

To display the contents of a directory, use the **dir** command.

dir [*filesystem***:**] [*//server/*] [*directory*]

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **debug**, **log**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.

Note There can be no spaces in the *filesystem://server/directory* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

Displays the contents of the current working directory.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **dir** command displays a listing of the files in the specified directory. For each file, it lists the size of the file in bytes, the last modified time of the file, and the filename of the file. This command then displays the usage statistics for the file system.

Use the **pwd** command to verify the current working directory.

Use the **cd** command to change the current working directory.

Examples

This example shows how to display the contents of the root directory in bootflash:

```
switch# dir bootflash:
```

This example shows how to display the contents of the current working directory:

```
switch# dir
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cd	Changes the current working directory.
delete	Deletes a file or directory.
pwd	Displays the name of the current working directory.
rmdir	Deletes a directory.

Send comments to nx5000-docfeedback@cisco.com

echo

To display a text string on the terminal, use the **echo** command.

echo [*text*]

Syntax Description

text	(Optional) Text string to display. The text string is alphanumeric, case sensitive, can contain spaces, and has a maximum length of 200 characters. The text string can also contain references to CLI variables.

Command Default

Blank line

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can use this command in a command script to display status information or prompts while the script is running.

Examples

This example shows how to display a blank line at the command prompt:

```
switch# echo
```

This example shows how to display a line of text at the command prompt:

```
switch# echo Script run at $(TIMESTAMP).
```

Related Commands

Command	Description
run-script	Runs command scripts.
show cli variables	Displays the CLI variables.

Send comments to nx5000-docfeedback@cisco.com

end

To end the current configuration session and return to EXEC mode, use the **end** command.

end

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command returns you to EXEC mode regardless of which configuration mode you are in. Use this command when you are done configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

This example shows how the **end** command is used to exit from interface configuration mode and return to EXEC mode. A **show** command is used to verify the configuration.

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport host
switch(config-if)# end
switch# show interface ethernet 1/1
```

Related Commands

Command	Description
exit (EXEC)	Terminates the active terminal session by logging off the router.
exit (global)	Exits from the current configuration mode.

Send comments to nx5000-docfeedback@cisco.com

exec-timeout

To configure the inactive session timeout on the console port or the virtual terminal, use the **exec-timeout** command. To revert to the default, use the **no** form of this command.

exec-timeout *minutes*

no exec-timeout

Syntax Description

minutes	Number of minutes. The range is from 0 to 525600. A setting of 0 minutes disables the timeout.

Command Default

Timeout is disabled.

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the inactive session timeout for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# exec-timeout 30
```

This example shows how to revert to the default inactive session timeout for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no exec-timeout
```

This example shows how to configure the inactive session timeout for the virtual terminal:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# exec-timeout 30
```

This example shows how to revert to the default inactive session timeout for the virtual terminal:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# no exec-timeout
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
line console	Enters the console terminal configuration mode.
line vty	Enters the virtual terminal configuration mode.
show running-config	Displays the running configuration.

Send comments to nx5000-docfeedback@cisco.com

exit (EXEC)

To close an active terminal session by logging off the switch, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how the **exit (global)** command is used to move from configuration mode to EXEC mode and the **exit** (EXEC) command is used to log off (exit the active session):

```
switch(config)# exit
switch# exit
```

Related Commands

Command	Description
end	Ends your configuration session by exiting to EXEC mode.
exit (global)	Exits from the current configuration mode to the next highest configuration mode.

Send comments to nx5000-docfeedback@cisco.com

exit (global)

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

All configuration modes

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **exit** command in configuration mode to return to EXEC mode. Use the **exit** command in interface, VLAN, or zone configuration mode to return to configuration mode. At the highest level, EXEC mode, the **exit** command will exit the EXEC mode and disconnect from the switch (see the description of the **exit (EXEC)** command for details).

Examples

This example shows how to exit from the interface configuration mode and to return to the configuration mode:

```
switch(config-if)# exit
switch(config)#
```

Related Commands

Command	Description
end	Ends your configuration session by exiting to privileged EXEC mode.
exit (EXEC)	Terminates the active terminal session by logging off the router.

Send comments to nx5000-docfeedback@cisco.com

feature fcoe

To enable virtual and native Fibre Channel interfaces after installing the FC_FEATURES_PKG license, use the **feature fcoe** command. To disable Fibre Channel interfaces and return the FC_FEATURES_PKG license to the license manager software, use the **no** form of this command.

feature fcoe

no feature fcoe

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must save the configuration, and then reboot the switch to enable or disable the FCoE feature.

Examples

This example shows how to enable FCoE on the switch:

```
switch(config)# feature fcoe
```

Related Commands

Command	Description
fcoe	Configures FCoE parameters.
show feature	Displays whether or not FCoE is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature fex

To enable Fabric Extender (FEX) features on the switch, use the **feature fex** command. To disable FEX, use the **no** form of this command.

feature fex

no feature fex

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to enable FEX features on the switch:

```
switch(config)# feature fex
switch(config)#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
show feature	Displays the features enabled or disabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature interface-vlan

To enable the creation of VLAN interfaces, use the **feature interface-vlan** command. To disable the VLAN interface feature, use the **no** form of this command.

feature interface-vlan

no feature interface-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN interfaces are disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature interface-vlan** command before you can create VLAN interfaces.

Examples

This example shows how to enable the interface VLAN feature on the switch:

```
switch(config)# feature interface-vlan
```

Related Commands

Command	Description
interface vlan	Creates a VLAN interface.
show feature	Displays whether or not VLAN interface is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature lacp

To enable Link Aggregation Control Protocol (LACP), which bundles a number of physical ports together to form a single logical channel, use the **feature lacp** command. To disable LACP on the switch, use the **no** form of this command.

feature lacp

no feature lacp

Syntax Description

This command has no arguments or keywords.

Command Default

LACP is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must remove all the LACP configuration parameters from all EtherChannels on the switch before you can disable LACP.

Even after you enable LACP globally, you do not have to run LACP on all EtherChannels on the switch. You enable LACP on each channel mode using the **channel-group mode** command.

Examples

This example shows how to enable LACP EtherChannels on the switch:

```
switch(config)# feature lacp
```

Related Commands

Command	Description
show lacp	Displays information on LACP.
show feature	Displays whether or not LACP is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature lldp

The Link Layer Discovery Protocol (LLDP), which is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network, is enabled on the switch by default.

Command Default

Enabled

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You cannot enable or disable LLDP on a Cisco Nexus 5000 Series switch. LLDP is enabled on the switch by default. However, the **feature lldp** command shows as part of the running configuration on the switch.

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices connected to the network.

To support non-Cisco devices and to allow for interoperability between other devices, the switch supports the Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

Examples

This example shows how to enable LLDP on the switch:

```
switch(config)# feature lldp
switch(config)#
```

This example shows how to disable LLDP on the switch:

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

Related Commands

Command	Description
lldp	Configures the global LLDP options on the switch.
lldp (Interface)	Configures the LLDP feature on an interface.
show feature	Displays whether or not LLDP is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature private-vlan

To enable private VLANs, use the **feature private-vlan** command. To return to the default settings, use the **no** form of this command.

feature private-vlan

no feature private-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

Private VLANs are disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The private VLAN commands are not available until you enable the private VLAN feature.

You cannot disable the private VLANs if there are operational ports on the switch that are in private VLAN mode.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

Examples

This example shows how to enable private VLAN functionality on the switch:

```
switch(config)# feature private-vlan
```

Related Commands

Command	Description
private-vlan	Configures a VLAN as either a community, isolated, or primary private VLAN.
show vlan private-vlan	Displays information on private VLANs. If the feature is not enabled, this command is not available.
show feature	Displays whether or not private VLAN is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature tacacs+

To enable TACACS+, use the **feature tacacs+** command. To disable TACACS+, use the **no** form of this command.

feature tacacs+

no feature tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

Note When you disable TACACS+, the Cisco NX-OS software removes the TACACS+ configuration.

Examples

This example shows how to enable TACACS+:

```
switch(config)# feature tacacs+
```

This example shows how to disable TACACS+:

```
switch(config)# no feature tacacs+
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ information.
show feature	Displays whether or not TACACS+ is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature udld

To enable the Cisco-proprietary Unidirectional Link Detection (UDLD) protocol, which allows ports that are connected through fiber optics or copper Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists, use the **feature udld** command. To disable UDLD on the switch, use the **no** form of this command.

feature udld

no feature udld

Syntax Description

This command has no arguments or keywords.

Command Default

UDLD is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Examples

This example shows how to enable UDLD on the switch:

```
switch(config)# feature udld
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.
show feature	Displays whether or not UDLD is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

feature vpc

To enable virtual port channel (vPC), which allows links that are physically connected to two different Cisco Nexus 5000 Series devices to appear as a single port channel to a third device, use the **feature vpc** command. To disable vPC on the switch, use the **no** form of this command.

feature vpc

no feature vpc

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

In a vPC configuration, the third device can be a Cisco Nexus 2000 Series Fabric Extender or a switch, server, or any other networking device.

Examples

This example shows how to enable vPC on the switch:

```
switch(config)# feature vpc
```

Related Commands

Command	Description
show vpc	Displays the vPC configuration status.
show feature	Displays whether or not vPC is enabled on the switch.

Send comments to nx5000-docfeedback@cisco.com

find

To find filenames beginning with a character string, use the **find** command.

find *filename-prefix*

Syntax Description

filename-prefix	First part or all of a filename. The filename prefix is case sensitive.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **find** command searches all subdirectories under the current working directory. You can use the **cd** and **pwd** commands to navigate to the starting directory.

Examples

This example shows how to display filenames beginning with “n5000”:

```
switch# find n5000
```

Related Commands

Command	Description
cd	Changes the current working directory.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

format

To format the bootflash device, which erases its contents and restores it to its factory-shipped state, use the **format** command.

format bootflash:

Syntax Description

bootflash:	Specifies the name of the bootflash file system.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to format the bootflash device:

```
switch# format bootflash:
```

Related Commands

Command	Description
cd	Changes the current working directory.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

gunzip

To uncompress a compressed file, use the **gunzip** command.

gunzip [*filesystem***:**] [*//server/*] [*directory*] *filename*

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the file to uncompress. The filename is case sensitive.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The compressed filename must have the .gz extension.

The Cisco NX-OS software uses Lempel-Ziv 1977 (LZ77) coding for compression.

Examples

This example shows how to uncompress a compressed file:

```
switch# gunzip run_cnfg.cfg.gz
```

Related Commands

Command	Description
dir	Displays the directory contents.
gzip	Compresses a file.

Send comments to nx5000-docfeedback@cisco.com

gzip

To compress a file, use the **gzip** command.

gzip [*filesystem***:**] [*//server/*] [*directory*] *filename*

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the file to compress. The filename is case sensitive.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

After you run this command, the named file is replaced with a compressed file that has the .gz extension added to its filename.

The Cisco NX-OS software uses Lempel-Ziv 1977 (LZ77) coding for compression.

Examples

This example shows how to compress a file:

```
switch# gzip run_cnfg.cfg
```

Related Commands

Command	Description
dir	Displays the directory contents.
gunzip	Uncompresses a compressed file.

Send comments to nx5000-docfeedback@cisco.com

hostname

To configure the hostname for the switch, use the **hostname** command. To revert to the default, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	Hostname for the switch. The name is alphanumeric, case sensitive, can contain special characters, and can have a maximum of 32 characters.

Command Default

"switch" is the default hostname.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software uses the hostname in command-line interface (CLI) prompts and in default configuration filenames.

The **hostname** command performs the same function as the **switchname** command.

Examples

This example shows how to configure the hostname for a Cisco Nexus 5000 Series switch:

```
switch# configure terminal
switch(config)# hostname Engineering2
Engineering2(config)#
```

This example shows how to revert to the default hostname:

```
Engineering2# configure terminal
Engineering2(config)# no hostname
switch(config)#
```

Related Commands

Command	Description
show hostname	Displays the switch hostname.
show switchname	Displays the switch hostname.
switchname	Configures the switch hostname.

Send comments to nx5000-docfeedback@cisco.com

install all

To install the kickstart and system images on a Cisco Nexus 5000 Series switch, use the **install all** command.

install all [**kickstart** *kickstart-url*] [**system** *system-url*]

Syntax Description

kickstart	(Optional) Specifies the kickstart image file.
kickstart-url	Full address of the kickstart image file. The name is case sensitive.
system	(Optional) Specifies the system image file.
system-url	Full address of the system image file. The name is case sensitive.

Command Default

If you do not enter any parameters, the boot variable values are used.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The format of the kickstart and system URLs varies according to the file system, directory, and file location.

The following tables list URL prefix keywords by the file system type. If you do not specify a URL prefix keyword, the router looks for a file in the current directory.

Table 1-4 lists URL prefix keywords for local writable storage file systems. Table 1-5 lists the URL prefix keywords for remote file systems. For remote file systems, if it is not otherwise specified, the path is the default for the user on the remote server.

Table 1-4 URL Prefix Keywords for Local Writable Storage File Systems

Keyword	Source or Destination
bootflash:[*//server/*]	Source URL for boot flash memory. The *server* argument value is **module-1**, **sup-1**, **sup-active**, or **sup-local**.
modflash:[*//server/*]	Source URL of an external flash file system. The *server* argument value is **module-1**, **sup-1**, **sup-active**, or **sup-local**.
volatile:[*//server/*]	Source URL of the default internal file system. Any files or directories stored in this file system are erased when the switch reboots. The *server* argument value is **module-1**, **sup-1**, **sup-active**, or **sup-local**.

Send comments to nx5000-docfeedback@cisco.com

Table 1-5 URL Prefix Keywords for Remote File Systems

Keyword	Source or Destination
ftp:	Source URL for a FTP network server. The syntax for this alias is as follows: **ftp:**[//*server*][/*path*]/*filename*
scp:	Source URL for a network server that supports Secure Shell (SSH) and uses the secure copy protocol (scp). The syntax is as follows: **scp:**[//[*username***@**]*server*][/*path*]/*filename*
sftp:	Source URL for an SSH FTP (SFTP) network server. The syntax is as follows: **sftp:**[//[*username*@]*server*][/*path*]/*filename*
tftp:	Source URL for a TFTP network server. The syntax is as follows: **tftp:**[//*server*[:*port*]][/*path*]/*filename*

If you do not enter the information about the server or username when downloading and installing the image files from a remote server, you are prompted for the information.

This command sets the kickstart and system boot variables and copies the image files to the redundant supervisor module.

The **install all** command upgrades the switch software and also upgrades the Fabric Extender software of all attached chassis. The Fabric Extender remains online passing traffic while the software is copied. Once the software images have successfully been installed, the parent switch and the Fabric Extender chassis are rebooted automatically to maintain the software version compatibility between the parent switch and the Fabric Extender.

You can use the **install all** command to downgrade the Cisco NX-OS software on the switch. To determine if the downgrade software is compatible with the current configuration on the switch, use the **show incompatibility system** command and resolve any configuration incompatibilities.

Examples

This example shows how to install the Cisco NX-OS software from the bootflash: directory:

```
switch# install all kickstart bootflash:nx-os_kick.bin system bootflash:nx-os_sys.bin
```

This example shows how to install the Cisco NX-OS software using the values configured in the kickstart and system boot variables:

```
switch# configure terminal
switch(config)# boot kickstart bootflash:nx-os_kick.bin
switch(config)# boot system bootflash:nx-os_sys.bin
switch(config)# exit
switch# copy running-config startup-config
switch# install all
```

This example shows how to install the Cisco NX-OS software from an SCP server:

```
switch# install all kickstart scp://adminuser@192.168.1.1/nx-os_kick.bin system
bootflash:scp://adminuser@192.168.1.1/nx-os_sys.bin
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
reload	Reloads the device with new Cisco NX-OS software.
show incompatibility system	Displays configuration incompatibilities between Cisco NX-OS system software images.
show version	Displays information about the software version.

Send comments to nx5000-docfeedback@cisco.com

install license

To install a license, use the **install license** command.

install license [*filesystem***:**] [*//server/*] [*directory*] *src-filename* [*target-filename*]

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash** or **volatile**.
//server/	(Optional) Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
src-filename	Name of the source license file.
target-filename	(Optional) Name of the target license file.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

All licenses for the Cisco Nexus 5000 Series switches are factory installed. Manual installation is not required.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If a target filename is provided after the source location, the license file is installed with that name. Otherwise, the filename in the source URL is used. This command also verifies the license file before installing it.

Examples

This example shows how to install a file named license-file that resides in the bootflash: directory:

```
switch# install license bootflash:license-file
```

Related Commands

Command	Description
show license	Displays license information.
show license host-id	Displays the serial number of the chassis to use for licensing.
show license usage	Displays license usage information.

Send comments to nx5000-docfeedback@cisco.com

line console

To specify the console port and enter console port configuration mode, use the **line console** command.

line console

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console line only from a console port session.

Examples

This example shows how to enter console port configuration mode:

```
switch# configure terminal
switch(config)# line console
switch(config-console)#
```

Related Commands

Command	Description
databits	Configures the number of data bits in a character for a port.
exec-timeout	Configures the inactive terminal timeout for a port.
modem	Configures the modem settings for a port.
parity	Configures the parity settings for a port.
show line	Displays information about the console port configuration.
speed	Configures the transmit and receive speed for a port.
stopbits	Configures the stop bits for a port.

Send comments to nx5000-docfeedback@cisco.com

line vty

To specify the virtual terminal and enter line configuration mode, use the **line vty** command.

line vty

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enter console port configuration mode:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)#
```

Related Commands

Command	Description
exec-timeout	Configures the inactive terminal timeout for a port.
session-limit	Configures the maximum number of the concurrent virtual terminal sessions.
show line	Displays information about the console port configuration.

Send comments to nx5000-docfeedback@cisco.com

modem in

To enable the modem connection on the console port, use the **modem in** command. To disable the modem connection, use the **no** form of this command.

modem in

no modem in

Syntax Description

This command has no arguments or keywords.

Command Default

Timeout is disabled.

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to enable a modem connection on the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# modem in
```

This example shows how to disable a modem connection on the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no modem in
```

Related Commands

Command	Description
line console	Enters console port configuration mode.
show line	Displays information about the console port configuration.

Send comments to nx5000-docfeedback@cisco.com

modem init-string

To download the initialization string to a modem connected to the console port, use the **modem init-string** command. To revert to the default, use the **no** form of this command.

modem init-string {**default** | **user-input**}

no modem init-string

Syntax Description

default	Downloads the default initialization string.
user-input	Downloads the user-input initialization string.

Command Default

The default initialization string is ATE0Q1&D2&C1S0=1\015.

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

The default initialization string ATE0Q1&D2&C1S0=1\015 is defined as follows:

- AT—Attention
- E0 (required)—No echo
- Q1—Result code on
- &D2—Normal data terminal ready (DTR) option
- &C1—Enable tracking the state of the data carrier
- S0=1—Pick up after one ring
- \015 (required)—Carriage return in octal

Use the **modem set-string** command to configure the user-input initialization string.

Examples

This example shows how to download the default initialization string to the modem connected to the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# modem init-string default
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to download the user-input initialization string to the modem connected to the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# modem init-string user-input
```

This example shows how to remove the initialization string to the modem connected to the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no modem init-string
```

Related Commands

Command	Description
line console	Enters console port configuration mode.
modem set-string	Configures the user-input initialization string for a modem.
show line	Displays information about the console port configuration.

Send comments to nx5000-docfeedback@cisco.com

modem set-string user-input

To configure the user-input initialization string to download to a modem connected to the console port, use the **modem set-string user-input** command. To revert to the default, use the **no** form of this command.

modem set-string user-input *string*

no modem set-string

Syntax Description

string	User-input string. This string is alphanumeric and case sensitive, can contain special characters, and has a maximum of 100 characters.

Command Default

None

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the user-input initialization string for the modem connected to the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

This example shows how to revert to the default user-input initialization string for the modem connected to the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no modem set-string
```

Related Commands

Command	Description
line console	Enters console port configuration mode.
modem init-string	Downloads the user-input initialization string to a modem.
show line	Displays information about the console port configuration.

Send comments to nx5000-docfeedback@cisco.com

move

To move a file from one directory to another, use the **move** command.

move {[*filesystem*:] [//*server*/] [*directory*] *source-filename*} [*filesystem*:] [//*server*/] [*directory*] [*destination-filename*]

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **debug**, **modflash**, or **volatile**.
//*server*/	(Optional) Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
source-filename	Name of the file to move. The filename is case sensitive.
destination-filename	(Optional) Name of the destination file. The filename is alphanumeric, case sensitive, and has a maximum of 64 characters.

Command Default

The default filename for the destination file is the same as the source file.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can make a copy of a file by using the **copy** command.

Tip You can rename a file by moving it within the same directory.

Examples

This example shows how to move a file to another directory:

```
switch# move file1 my_files/file2
```

This example shows how to move a file to another file system:

```
switch# move file1 volatile:
```

This example shows how to move a file to another supervisor module:

```
switch# move file1 bootflash://sup-1/file1.bak
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Makes a copy of a file.
delete	Deletes a file or directory.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

parity

To configure the parity for the console port, use the **parity** command. To revert to the default, use the **no** form of this command.

parity {**even** | **none** | **odd**}

no parity {**even** | **none** | **odd**}

Syntax Description

even	Specifies even parity.
none	Specifies no parity.
odd	Specifies odd parity.

Command Default

The **none** keyword is the default.

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the parity for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# parity even
```

This example shows how to revert to the default parity for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no parity even
```

Related Commands

Command	Description
show line	Displays information about the console port configuration.

Send comments to nx5000-docfeedback@cisco.com

ping

To determine the network connectivity to another network device, use the **ping** command.

ping {*dest-address* | *hostname*} [**count** {*number* | **unlimited**}] [**df-bit**] [**interval** *seconds*] [**packet-size** *bytes*] [**source** *src-address*] [**timeout** *seconds*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

dest-address	IPv4 address of the destination device. The format is *A.B.C.D*.
hostname	Hostname of the destination device. The hostname is case sensitive.
count	(Optional) Specifies the number of transmissions to send.
number	Number of pings. The range is from 1 to 655350. The default is 5.
unlimited	Allows an unlimited number of pings.
df-bit	(Optional) Enables the do-not-fragment bit in the IPv4 header. The default is disabled.
interval *seconds*	(Optional) Specifies the interval in seconds between transmissions. The range is from 0 to 60. The default is 1 second.
packet-size *bytes*	(Optional) Specifies the packet size in bytes to transmit. The range is from 1 to 65468. The default is 56 bytes.
source *scr-address*	(Optional) Specifies the source IPv4 address to use. The format is *A.B.C.D*. The default is the IPv4 address for the management interface of the device.
timeout *seconds*	(Optional) Specifies the nonresponse timeout interval in seconds. The range is from 1 to 60. The default is 2 seconds.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

For the default values, see the “Syntax Description” section for this command.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to determine connectivity to another network device:

```
switch# ping 192.168.2.246
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
ping6	Determines connectivity to another device using IPv6 addressing.
traceroute	Displays the routes that packets take when traveling to an IP address.

Send comments to nx5000-docfeedback@cisco.com

ping6

To determine the network connectivity to another device using IPv6 addressing, use the **ping6** command.

ping6 {*dest-address* | *hostname*} [**count** {*number* | **unlimited**}] [**interface** *intf-id*] [**interval** *seconds*] [**packet-size** *bytes*] [**source** *address*] [**timeout** *seconds*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

dest-address	Destination IPv6 address. The format is *A*:*B*::*C*:*D*.
hostname	Hostname of destination device. The hostname is case sensitive.
count	(Optional) Specifies the number of transmissions to send.
number	Number of pings. The range is from 1 to 655350. The default is 5.
unlimited	Allows an unlimited number of pings.
interface *intf-id*	(Optional) Specifies the interface to send the IPv6 packet. The valid interface types are Ethernet, loopback, EtherChannel, and VLAN.
interval *seconds*	(Optional) Specifies the interval in seconds between transmissions. The range is from 0 to 60. The default is 1 second.
packet-size *bytes*	(Optional) Specifies the packet size in bytes to transmit. The range is from 1 to 65468.
source *address*	(Optional) Specifies the source IPv6 address to use. The format is *A*:*B*::*C*:*D*. The default is the IPv6 address for the management interface of the device.
timeout *seconds*	(Optional) Specifies the nonresponse timeout interval in seconds. The range is from 1 to 60. The default is 2 seconds.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

For the default values, see the “Syntax Description” section for this command.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Examples

This example shows how to determine connectivity to another device using IPv6 addressing:

```
switch# ping6 2001:0DB8::200C:417A vrf management
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
ping	Determines connectivity to another device using IPv4 addressing.
traceroute6	Displays the routes that packets take when traveling to an IPv6 address.

Send comments to nx5000-docfeedback@cisco.com

reload

To reload the switch and all attached Fabric Extender chassis or a specific Fabric Extender, use the **reload** command.

reload {**all** | **fex** *chassis_ID*}

Syntax Description

all	Reboots the entire Cisco Nexus 5000 Series switch and all attached Fabric Extender chassis.
fex *chassis_ID*	Reboots a specific Fabric Extender chassis. The chassis ID is from 100 to 199.

Command Default

Reloads the Cisco Nexus 5000 Series switch.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	Support for the Cisco Nexus 2000 Series Fabric Extender was added.

Usage Guidelines

The **reload** command disrupts traffic on the switch and Fabric Extender.

Note The **reload** command does not save the running configuration. Use the **copy running-config startup-config** command to save the current configuration on the device.

Examples

This example shows how to reload the Cisco Nexus 5000 Series switch:

```
switch# copy running-config startup-config
switch# reload
This command will reboot the system. (y/n)?  [n] y
```

This example shows how to reload a Fabric Extender:

```
switch# reload fex 101
WARNING: This command will reboot FEX 101
Do you want to continue? (y/n) [n] y
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the current running configuration to the startup configuration.
show version	Displays information about the software version.

Send comments to nx5000-docfeedback@cisco.com

rmdir

To remove a directory, use the **rmdir** command.

rmdir [*filesystem***:** [*//server/*]] *directory*

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	Name of a directory to delete. The directory name is case sensitive.

Note There can be no spaces in the *filesystem://server/directory* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to remove a directory:

```
switch# rmdir my_files
```

Related Commands

Command	Description
cd	Changes the current working directory.
delete	Deletes a file or directory.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

run-script

To run a command script file at the command-line interface (CLI), use the **run-script** command.

run-script [*filesystem*:[//*module*/]][*directory*/]*filename*

Syntax Description

filesystem:	(Optional) Name of a file system. The name is case sensitive.
//*module*/	(Optional) Identifier for a supervisor module. Valid values are **sup-active**, **sup-local**, **sup-remote**, or **sup-standby**. The identifiers are case sensitive.
directory/	(Optional) Name of a directory. The name is case sensitive.
filename	Name of the command file. The name is case sensitive.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must create the command file on a remote device and download it to the Cisco Nexus 5000 Series switch using the **copy** command.

Examples

This example shows how to run a command script file:

```
switch# run-script script-file
```

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Copies files.
dir	Displays the directory contents.
echo	Displays a test string on the terminal.
pwd	Displays the name of the current working directory.
sleep	Causes the CLI to pause for a defined number of seconds.

Send comments to nx5000-docfeedback@cisco.com

save

To save the current configuration session to a file, use the **save** command.

save *location*

Syntax Description

location	Location of the file. The location can be in bootflash or volatile. The file name can be any alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Session configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Examples

This example shows how to save a configuration session to a file in bootflash:

```
switch# configure session MySession
switch(config-s)# save bootflash:sessions/MySession
```

Related Commands

Command	Description
configure session	Creates or modifies a configuration session.
delete	Deletes a file from a location.

Send comments to nx5000-docfeedback@cisco.com

send

To send a message to the active user sessions, use the **send** command.

send [**session** *line*] *text*

Syntax Description

session *line*	(Optional) Specifies a user session.
text	Text string. The text string can be up to 80 alphanumeric characters and is case sensitive.

Command Default

Sends a message to all active user sessions.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can use the **show users** command to display information about the active user sessions.

Examples

This example shows how to send a message to all active user sessions on the switch:

```
switch# send The system will reload in 15 minutes!
The system will reload in 15 minutes!
```

This example shows how to send a message to a specific user session:

```
switch# send session pts/0 You must log off the switch.
```

Related Commands

Command	Description
show users	Displays the active user sessions on the switch.

Send comments to nx5000-docfeedback@cisco.com

setup

To enter the basic device setup dialog, use the **setup** command.

setup [**ficon**]

Syntax Description		
	ficon	(Optional) Runs the basic ficon setup command facility.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines The setup script uses the factory-default values, not the values that you have configured. You can exit the dialog at any point by pressing **Ctrl-C**.

Examples This example shows how to enter the basic device setup script:

```
switch# setup
```

Related Commands	Command	Description
	show running-config	Displays the running configuration.

Send comments to nx5000-docfeedback@cisco.com

session-limit

To configure the maximum number of the concurrent virtual terminal sessions on a device, use the **session-limit** command. To revert to the default, use the **no** form of this command.

session-limit *sessions*

no session-limit *sessions*

Syntax Description

sessions	Maximum number of sessions. The range is from 1 to 64.

Command Default

32 sessions

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure the maximum number of concurrent virtual terminal sessions:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# session-limit 48
```

This example shows how to revert to the default maximum number of concurrent virtual terminal sessions:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# no session-limit 48
```

Related Commands

Command	Description
line vty	Enters the virtual terminal configuration mode.
show running-config	Displays the running configuration.

Send comments to nx5000-docfeedback@cisco.com

show banner motd

To display the message-of-the-day (MOTD) banner, use the **show banner motd** command.

show banner motd

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the MOTD banner:

```
switch# show banner motd
Unauthorized access is prohibited!
```

Related Commands

Command	Description
banner motd	Configures the MOTD banner.

Send comments to nx5000-docfeedback@cisco.com

show boot

To display the boot variable configuration, use the **show boot** command.

show boot [**variables**]

Syntax Description

variables	(Optional) Displays a list of boot variables.

Command Default

Displays all configured boot variables.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all configured boot variables:

```
switch# show boot
```

This example shows how to display the list of boot variable names:

```
switch# show boot variables
```

Related Commands

Command	Description
boot	Configures the boot variable for the kickstart or system image.

Send comments to nx5000-docfeedback@cisco.com

show cli alias

To display the command alias configuration, use the **show cli alias** command.

show cli alias [**name** *alias-name*]

Syntax Description		
	name *alias-name*	(Optional) Specifies the name of a command alias. The alias name is not case sensitive.

Command Default Displays all configured command alias variables.

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display all configured command aliases:

```
switch# show cli alias
```

This example shows how to display a specific command alias:

```
switch# show cli alias name ethint
```

Related Commands	Command	Description
	cli alias name	Configures command aliases.

Send comments to nx5000-docfeedback@cisco.com

show cli history

To display the command history, use the **show cli history** command.

show cli history [*lines*] [**unformatted**]

Syntax Description		
	lines	(Optional) Last number of lines from the end of the command history.
	unformatted	(Optional) Displays the commands without line numbers or time stamps.

Command Default Displays the entire formatted history.

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display all of the command history:

```
switch# show cli history
```

This example shows how to display the last 10 lines of the command history:

```
switch# show cli history 10
```

This example shows how to display unformatted command history:

```
switch# show cli history unformatted
```

Related Commands	Command	Description
	clear cli history	Clears the command history.

Send comments to nx5000-docfeedback@cisco.com

show cli variables

To display the configuration of the command-line interface (CLI) variables, use the **show cli variables** command.

show cli variables

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the CLI variables:

```
switch# show cli variables
```

Related Commands

Command	Description
cli var name	Configures CLI variables.

Send comments to nx5000-docfeedback@cisco.com

show clock

To display the current date and time, use the **show clock** command.

show clock [**detail**]

Syntax Description

detail	(Optional) Displays the summer-time (daylight saving time) offset configuration.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the current clock setting:

```
switch# show clock
```

This example shows how to display the current clock setting and the summer-time (daylight saving time) configuration:

```
switch# show clock detail
```

Related Commands

Command	Description
clock set	Sets the clock time.
clock summer-time	Configures the summer-time (daylight saving time) offset.

Send comments to nx5000-docfeedback@cisco.com

show configuration session

To display information about configuration sessions, use the **show configuration session** command.

show configuration session [*session-name* | **status** | **summary**]

Syntax Description

session-name	(Optional) Configuration session name. The name can be a maximum of 64 alphanumeric characters.
status	(Optional) Displays the status of the configuration session.
summary	(Optional) Displays summary information of the active configuration sessions.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1)	This command was introduced.

Examples

This example shows how to display information about a specific configuration session:

```
switch# show configuration session mySession1
config session name mySession1
0001  ip access-list myACL
0002  permit icmp any any
0003  statistics per-entry
switch#
```

This example shows how to display the status of the active configuration session:

```
switch# show configuration session status
==============================================================================
Session Name          : mySession1
Last Action           : Validate
Last Action Status    : Success
Last Action Reason    : -NA-
Last Action Timestamp : 19:03:49 UTC Sep 06 2009
==============================================================================

switch#
```

This example shows how to display the summary information of the active configuration sessions:

```
switch# show configuration session summary
Session Manager Database:
------------------------------------------------------------------
Name                    Session Owner           Creation Time
------------------------------------------------------------------
mySession1              root                    18:09:03 UTC Sep 06 2009
```

Send comments to nx5000-docfeedback@cisco.com

```
Number of active configuration sessions = 1
switch#
```

Related Commands

Command	Description
configure session	Creates a configuration session.

Send comments to nx5000-docfeedback@cisco.com

show copyright

To display the Cisco NX-OS software copyright information, use the **show copyright** command.

show copyright

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the Cisco NX-OS copyright information:

```
switch# show copyright
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2010, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show debug logfile

To display the contents of the debug logfile, use the **show debug logfile** command.

show debug logfile *filename*

Syntax Description

filename	Name of the debug log file.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The log files are located in the log: file system.

Examples

This example shows how to display the contents of a debug log file:

```
switch# show debug logfile dmesg
```

Related Commands

Command	Description
debug logfile	Configures the debug log file.

Send comments to nx5000-docfeedback@cisco.com

show environment

To display information about the hardware environment status, use the **show environment** command.

show environment [**fan** | **power** | **temperature**]

Syntax Description

fan	(Optional) Displays information about the fan environment.
power	(Optional) Displays information about the power capacity and distribution.
temperature	(Optional) Displays information about the temperature environment.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information about the hardware environment:

```
switch# show environment


Fan:
----------------------------------------------------
Fan             Model                Hw         Status
----------------------------------------------------
Chassis-1       N5K-C5020-FAN        --         ok
Chassis-2       --                   --         absent
Chassis-3       N5K-C5020-FAN        --         ok
Chassis-4       N5K-C5020-FAN        --         ok
Chassis-5       N5K-C5020-FAN        --         ok
PS-1            N5K-PAC-1200W        --         failure
PS-2            N5K-PAC-1200W        --         ok


Temperature
-----------------------------------------------------------------------
Module   Sensor     MajorThresh   MinorThres   CurTemp     Status
                    (Celsius)     (Celsius)    (Celsius)
-----------------------------------------------------------------------
1        Outlet-1   60            50           41          ok
1        Outlet-2   60            50           44          ok
1        Outlet-3   60            50           36          ok
1        Outlet-4   60            50           39          ok
1        Intake-1   50            40           26          ok
1        Intake-2   50            40           25          ok
1        Intake-3   50            40           25          ok
1        Intake-4   50            40           25          ok
1        PS-1       60            50           20          ok
1        PS-2       60            50           27          ok
```

Send comments to nx5000-docfeedback@cisco.com

```
3        Outlet-1   60            50           30          ok
2        Outlet-1   60            50           32          ok


Power Supply:
Voltage: 12 Volts
------------------------------------------------------
PS  Model               Power       Power     Status
                        (Watts)     (Amp)
------------------------------------------------------
1   --                      --        --      fail/shutdown
2   N5K-PAC-1200W       1200.00    100.00     ok


Mod Model                  Power     Power       Power     Power       Status
                           Requested Requested   Allocated Allocated
                           (Watts)   (Amp)       (Watts)   (Amp)
--- -----------___--------  -------   ----------  --------- ----------  --------
--
1    N5K-C5020P-BF-SUP     625.20    52.10       625.20    52.10       powered-
up
2    N5K-M1600             54.00     4.50        54.00     4.50        powered-
up
3    N5K-M1008             9.96      0.83        9.96      0.83        powered-
up


Power Usage Summary:
--------------------
Power Supply redundancy mode:                Redundant
Power Supply redundancy operational mode:    Non-redundant

Total Power Capacity                           1200.00 W

Power reserved for Supervisor(s)                625.20 W
Power currently used by Modules                  63.96 W

                                               -------------
Total Power Available                           510.84 W
                                               -------------
switch#
```

This example shows how to display information about the power environment:

```
switch# show environment power


Power Supply:
Voltage: 12 Volts
------------------------------------------------------
PS  Model               Power       Power     Status
                        (Watts)     (Amp)
------------------------------------------------------
1   --                      --        --      fail/shutdown
2   N5K-PAC-1200W       1200.00    100.00     ok


Mod Model                  Power     Power       Power     Power       Status
                           Requested Requested   Allocated Allocated
                           (Watts)   (Amp)       (Watts)   (Amp)
--- -----------___--------  -------   ----------  --------- ----------  --------
--
1    N5K-C5020P-BF-SUP     625.20    52.10       625.20    52.10       powered-
up
```

Send comments to nx5000-docfeedback@cisco.com

```
2    N5K-M1600              54.00     4.50        54.00     4.50        powered-
up
3    N5K-M1008              9.96      0.83        9.96      0.83        powered-
up


Power Usage Summary:
--------------------
Power Supply redundancy mode:                 Redundant
Power Supply redundancy operational mode:     Non-redundant

Total Power Capacity                             1200.00 W

Power reserved for Supervisor(s)                  625.20 W
Power currently used by Modules                    63.96 W

                                                -------------
Total Power Available                             510.84 W
                                                -------------
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show feature

To display the status of features on a switch, use the **show feature** command.

show feature

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the state of all features on a switch:

```
switch# show feature
Feature Name          Instance  State
--------------------  --------  --------
cimserver             1         disabled
fabric-binding        1         disabled
fc-port-security      1         disabled
fcoe                  1         enabled
fcsp                  1         disabled
fex                   1         enabled
fport-channel-trunk   1         disabled
http-server           1         enabled
interface-vlan        1         enabled
lacp                  1         enabled
lldp                  1         enabled
npiv                  1         disabled
npv                   1         disabled
port_track            1         disabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
udld                  1         enabled
vpc                   1         enabled
vtp                   1         disabled
switch#
```

Related Commands

Command	Description
feature	Enables or disables a feature on the switch.

Send comments to nx5000-docfeedback@cisco.com

show file

To display the contents of a file on the local memory, use the **show file** command.

show file [*filesystem***:**] [*//server/*] [*directory*] *filename*

Syntax Description

filesystem:	(Optional) Name of the file system. Valid values are **bootflash**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the file to delete. The filename is case sensitive.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the contents of a file:

```
switch# show file ent-mod.lic
```

If the file that you want to display is a directory, the command will return an error message:

```
switch# show file bootflash:///routing-sw
/bin/showfile: /bootflash/routing-sw: Is a directory
```

Related Commands

Command	Description
cd	Changes the current working directory.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

show hardware internal

To display information about the physical device hardware, use the **show hardware internal** command.

show hardware internal

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information about the physical device hardware:

```
switch# show hardware internal
```

Related Commands

Command	Description
show inventory	Displays hardware inventory information.
show module	Displays information about the modules.

Send comments to nx5000-docfeedback@cisco.com

show hostname

To display the hostname for the switch, use the **show hostname** command.

show hostname

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show switchname** command also displays the switch hostname.

Examples

This example shows how to display the hostname for the switch:

```
switch# show hostname
switch
switch#
```

Related Commands

Command	Description
hostname	Configures the hostname for the switch.
show switchname	Displays the hostname.
switchname	Configures the hostname for the switch.

Send comments to nx5000-docfeedback@cisco.com

show incompatibility system

To display the configuration incompatibilities between the running system image and an earlier system image prior to downgrading the Cisco NX-OS software, use the **show incompatibility system** command.

show incompatibility system {*filesystem*: //*server*/ [*directory*] *filename*}

Syntax Description

filesystem:	Name of the file system. Valid values are **bootflash** or **volatile**.
//*server*/	Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the file to compare with the loaded software image. The filename is case sensitive.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configuration incompatibilities:

```
switch# show incompatibility system bootflash://sup-local/old_image.bin
```

Related Commands

Command	Description
install all	Installs the kickstart and system images.
reload	Reloads the device with the new Cisco NX-OS software.
show version	Displays information about the software version.

Send comments to nx5000-docfeedback@cisco.com

show install all

To display information related to the operation of the **install all** command, use the **show install all** command.

show install all {**failure-reason** | **impact** [**kickstart** | **system**] | **status**}

Syntax Description

failure-reason	Displays the software installation failure reason.
impact	Displays the impact of installing the images referred to in the boot variables.
kickstart	(Optional) Displays the impact of installing the kickstart image referred to in the kickstart boot variable.
system	(Optional) Displays the impact of installing the system image referred to in the kickstart boot variable.
status	Displays the status of the software installation process.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the installation failure reason:

```
switch# show install all failure-reason
No install all failure-reason
switch#
```

This example shows how to display the impact of installing new images:

```
switch# show install all impact
```

This example shows how to display the status of the software installation process:

```
switch# show install all status
There is an on-going installation...
Enter Ctrl-C to go back to the prompt.

switch#
```

Related Commands

Command	Description
install all	Installs the software on the physical device.
show boot	Displays the boot variable configuration.

Send comments to nx5000-docfeedback@cisco.com

show inventory

To display the physical inventory information for the switch hardware, use the **show inventory** command.

show inventory [**fex** *chassis_ID*]

Syntax Description

fex *chassis_ID*	(Optional) Specifies the Fabric Extender chassis ID. The chassis ID is from 100 to 199.

Command Default

Displays all hardware inventory information.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	This command was modified to provide Fabric Extender support.

Examples

This example shows how to display the switch hardware inventory information:

```
switch# show inventory
NAME: "Chassis", DESCR: "Nexus5020 Chassis"
PID: N5K-C5020P-BF     , VID: V04 , SN: SSI13390FZT

NAME: "Module 1", DESCR: "40x10GE/Supervisor"
PID: N5K-C5020P-BF     , VID: V04 , SN: JAF1344BHNK

NAME: "Module 2", DESCR: "6x10GE Ethernet Module"
PID: N5K-M1600         , VID: V01 , SN: JAB1228018M

NAME: "Module 3", DESCR: "8x1/2/4G FC Module"
PID: N5K-M1008         , VID: V01 , SN: JAB1231020C

NAME: "Fan 1", DESCR: "Chassis fan module"
PID: N5K-C5020-FAN     , VID: N/A , SN: N/A

NAME: "Fan 3", DESCR: "Chassis fan module"
PID: N5K-C5020-FAN     , VID: N/A , SN: N/A

NAME: "Fan 4", DESCR: "Chassis fan module"
PID: N5K-C5020-FAN     , VID: N/A , SN: N/A

NAME: "Fan 5", DESCR: "Chassis fan module"
PID: N5K-C5020-FAN     , VID: N/A , SN: N/A

NAME: "Power supply 1", DESCR: "AC power supply"
PID: N5K-PAC-1200W     , VID: V01 , SN: DTM134200L5

NAME: "Power supply 2", DESCR: "AC power supply"
PID: N5K-PAC-1200W     , VID: V01 , SN: DTM134200L4
```

Send comments to nx5000-docfeedback@cisco.com

```
NAME: "FEX 100 CHASSIS", DESCR: "N2K-C2148T-1GE  CHASSIS"
PID: N2K-C2148T-1GE    , VID: V01 , SN: FOX1252GQJR

NAME: "FEX 100 Module 1", DESCR: "Fabric Extender Module: 48x1GE, 4X10GE Supervi
sor"
PID: N2K-C2148T-1GE    , VID: V01 , SN: JAF1302ABDP

NAME: "FEX 100 Fan 1", DESCR: "Fabric Extender Fan module"
PID: N2K-C2148-FAN     , VID: N/A , SN: N/A

NAME: "FEX 100 Power Supply 1", DESCR: "Fabric Extender AC power supply"
PID: N2K-PAC-200W      , VID: V01 , SN: PAC12493LQX

NAME: "FEX 100 Power Supply 2", DESCR: "Fabric Extender AC power supply"
--More--
switch#
```

This example shows how to display the hardware inventory information for an attached Fabric Extender:

```
switch# show inventory fex 101
NAME: "FEX 100 CHASSIS", DESCR: "N2K-C2148T-1GE  CHASSIS"
PID: N2K-C2148T-1GE    , VID: V01 , SN: FOX1252GQJR

NAME: "FEX 100 Module 1", DESCR: "Fabric Extender Module: 48x1GE, 4X10GE Supervi
sor"
PID: N2K-C2148T-1GE    , VID: V01 , SN: JAF1302ABDP

NAME: "FEX 100 Fan 1", DESCR: "Fabric Extender Fan module"
PID: N2K-C2148-FAN     , VID: N/A , SN: N/A

NAME: "FEX 100 Power Supply 1", DESCR: "Fabric Extender AC power supply"
PID: N2K-PAC-200W      , VID: V01 , SN: PAC12493LQX

NAME: "FEX 100 Power Supply 2", DESCR: "Fabric Extender AC power supply"
PID: N5K-PAC-200W      , VID: 00V0, SN: PAC12423L1Q

switch#
```

Related Commands

Command	Description
show hardware internal	Displays information about the physical hardware.
show module	Displays information about the modules.

Send comments to nx5000-docfeedback@cisco.com

show license

To display license information, use the **show license** command.

show license [**brief** | **file** *filename*]

Syntax Description

brief	(Optional) Displays a list of license files installed on a device.
file *filename*	(Optional) Displays information for a specific license file.

Command Default

Displays information about the installed licenses.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display a specific license installed on the switch:

```
switch# show license file fc5020.lic
```

This example shows how to display a list of license files installed on a device:

```
switch# show license brief
fcoelicense.lic
switch#
```

This example shows how to display all licenses installed on a device:

```
switch# show license
fcoelicense.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ENTERPRISE_PKG cisco 1.0 permanent uncounted \
        VENDOR_STRING=<LIC_SOURCE>MDS_SWIFT</LIC_SOURCE><SKU>N5020-SSK9=</SKU> \
        HOSTID=VDH=SSI13390FZT \
        NOTICE="<LicFileID>20100611101827012</LicFileID><LicLineID>1</LicLineID>
 \
        <PAK></PAK>" SIGN=877DB4A06E0C
INCREMENT FC_FEATURES_PKG cisco 1.0 permanent uncounted \
        VENDOR_STRING=<LIC_SOURCE>MDS_SWIFT</LIC_SOURCE><SKU>N5020-SSK9=</SKU> \
        HOSTID=VDH=SSI13390FZT \
        NOTICE="<LicFileID>20100611101827012</LicFileID><LicLineID>2</LicLineID>
 \
        <PAK></PAK>" SIGN=A075D610878C

switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
install license	Installs a license.
show license host-id	Displays the serial number of the chassis to use for licensing.
show license usage	Displays license usage information.

Send comments to nx5000-docfeedback@cisco.com

show license host-id

To display the serial number (host ID) of the switch chassis to use for licensing, use the **show license host-id** command.

show license host-id

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The serial number is the entire string that appears after the colon (:) as shown in the example.

Examples

This example shows how to display the host ID, required to request node-locked licenses:

```
switch# show license host-id
License hostid: VDH=FLC12300568
switch#
```

Related Commands

Command	Description
install license	Installs a license.
show license	Displays license information.
show license usage	Displays license usage information.

Send comments to nx5000-docfeedback@cisco.com

show license usage

To display license usage information, use the **show license usage** command.

show license usage [*PACKAGE*]

Syntax Description

PACKAGE	(Optional) List of licensed features in use for the specified license package.

Command Default

Displays license usage for the switch.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information about the current license usage:

```
switch# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
FM_SERVER_PKG                 No    -   Unused             -
ENTERPRISE_PKG                Yes   -   Unused Never       -
FC_FEATURES_PKG               Yes   -   In use Never       -
--------------------------------------------------------------------------------
```

Table 1-6 describes the columns used in the **show license usage** command output.

Table 1-6 show license usage Columns

Column	Description
Feature	Name of the license package.
Ins	License installation status. “No” indicates that the license is not installed and “Yes” indicates that the license is installed.
Lic Count	License count. “-” indicates that the count is not used for this license package. A number in this field indicates that number of current usages of the license by features. This field is not supported.
Status	License status. “Unused” indicates that no features that require the license are enabled. “In use” indicates that one or more features are using the license.

Send comments to nx5000-docfeedback@cisco.com

Table 1-6 show license usage Columns (continued)

Column	Description
Expiry Date	License expiry date. The field is blank if the license is not installed. If the license is installed, the field displays “Never” to indicate that the license has no time limit or displays the date of expiry for the license.
Comments	Additional information. “Grace” with a time period remaining in days (“D”) and hours (:H”) indicates that the grace license is in use and “license missing” indicates that an error has occurred.

This example shows how to display a list of features in use for a specific license:

```
switch# show license usage FC_FEATURES_PKG
Application
-----------
PFM
-----------
switch#
```

Related Commands

Command	Description
install license	Installs a license.
show license	Displays license information.
show license host-id	Displays the serial number of the chassis to use for licensing.

Send comments to nx5000-docfeedback@cisco.com

show line

To display terminal port configuration information, use the **show line** command.

show line [**console** [**user-input-string**]]

Syntax Description

console	(Optional) Displays only information about the console port configuration.
user-input-string	(Optional) Displays the user-input initialization string.

Command Default

Displays information about the terminal port configuration.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.1(3)N1(1)	The **show line console user-input-string** was added.

Examples

This example shows how to display information about the terminal port configuration information:

```
switch# show line
line Console:
    Speed:        115200 baud
    Databits:     8 bits per byte
    Stopbits:     2 bit(s)
    Parity:       none
    Modem In: Disable
    Modem Init-String -
        default : ATE0Q1&D2&C1S0=1\015

line Aux:
    Speed:        9600 baud
    Databits:     8 bits per byte
    Stopbits:     1 bit(s)
    Parity:       none
    Modem In: Disable
    Modem Init-String -
        default : ATE0Q1&D2&C1S0=1\015
    Hardware Flowcontrol: ON

switch#
```

This example shows how to display only the information about the console port configuration:

```
switch# show line console
line Console:
    Speed:        115200 baud
    Databits:     8 bits per byte
    Stopbits:     2 bit(s)
    Parity:       none
    Modem In: Disable
```

Send comments to nx5000-docfeedback@cisco.com

```
    Modem Init-String -
        default : ATE0Q1&D2&C1S0=1\015

switch#
```

This example shows how to display the user-input initialization string for a modem:

```
switch# show line console user-input-string
Console's user-input string is ATE0Q1&D2&C1S0=3\015
switch#
```

Related Commands

Command	Description
line console	Enters the console port configuration mode.

Send comments to nx5000-docfeedback@cisco.com

show module

To display module information, use the **show module** command.

show module [*module-number* | **fex** [*chassis_ID* | **all**]]

Syntax Description

module-number	(Optional) Number of the module. The valid range is from 1 to 3.
fex	(Optional) Displays information about the attached Fabric Extender units.
chassis_ID	(Optional) Fabric Extender chassis ID. The chassis ID is from 100 to 199.
all	(Optional) Displays information about all the attached Fabric Extender units.

Command Default

Displays module information for all modules in the switch chassis.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	This command was modified to provide Fabric Extender support.

Examples

This example shows how to display information for all modules in the chassis:

```
switch# show module
Mod Ports  Module-Type                      Model                 Status
--- -----  -------------------------------- --------------------- ------------
1    40     40x10GE/Supervisor               N5K-C5020P-BF-SUP      active *
2    6      6x10GE Ethernet Module           N5K-M1600              ok
3    8      8x1/2/4G FC Module               N5K-M1008              ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    4.2(1)N2(1)     1.3     --
2    4.2(1)N2(1)     0.100   --
3    4.2(1)N2(1)     0.200   20:81:00:0d:ec:e7:df:40 to 20:88:00:0d:ec:e7:df:40

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    000d.ece7.df48 to 000d.ece7.df6f         JAF1344BHNK
2    000d.ece7.df70 to 000d.ece7.df77         JAB1228018M
3    000d.ece7.df78 to 000d.ece7.df7f         JAB1231020C
switch#
```

This example shows how to display information for a specific module:

```
switch# show module 2
Mod Ports  Module-Type                      Model                 Status
--- -----  -------------------------------- --------------------- ------------
2    6      6x10GE Ethernet Module           N5K-M1600              ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
```

Send comments to nx5000-docfeedback@cisco.com

```
---  -------------  ------  -------------------------------------------------
2    4.2(1)N2(1)     0.100   --

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
2    000d.ece7.df70 to 000d.ece7.df77         JAB1228018M
switch#
```

This example shows how to display information about an attached Fabric Extender:

```
switch# show module fex 100
FEX Mod Ports Card Type                          Model              Status.
--- --- ----- -------------------------------- ------------------ -----------
100 1   48    Fabric Extender 48x1GE Module      N2K-C2148T-1GE     present

FEX Mod Sw              Hw      World-Wide-Name(s) (WWN)
--- --- --------------  ------  -----------------------------------------------
100 1   4.2(1)N2(1)     1.0     --

FEX Mod  MAC-Address(es)                         Serial-Num
--- ---  --------------------------------------  ----------
100 1    000d.ecb1.ef00 to 000d.ecb1.ef2f        JAF1302ABDP
switch#
```

This example shows how to display information about all attached Fabric Extender units:

```
switch# show module fex all
FEX Mod Ports Card Type                          Model              Status.
--- --- ----- -------------------------------- ------------------ -----------
100 1   48    Fabric Extender 48x1GE Module      N2K-C2148T-1GE     present
150 1   48    Fabric Extender 48x1GE + 4x10G Mod N2K-C2248TP-1GE    present
151 1   48    Fabric Extender 48x1GE + 4x10G Mod N2K-C2248TP-1GE    present
170 1   32    Fabric Extender 32x10G BaseT + 8x1 0                  present
171 1   32    Fabric Extender 32x10G BaseT + 8x1 0                  present
198 1   32    Fabric Extender 32x10GE + 8x10G Mo N2K-C2232PP-10GE   present
199 1   32    Fabric Extender 32x10GE + 8x10G Mo N2K-C2232PP-10GE   present

FEX Mod Sw              Hw      World-Wide-Name(s) (WWN)
--- --- --------------  ------  -----------------------------------------------
100 1   4.2(1)N2(1)     1.0     --
150 1   4.2(1)N2(1)     3.4     --
151 1   4.2(1)N2(1)     3.2     --
170 1   4.2(1)N2(1)     1.0     --
171 1   4.2(1)N2(1)     1.0     --
198 1   4.2(1)N2(1)     3.4     --
199 1   4.2(1)N2(1)     3.5     --

FEX Mod  MAC-Address(es)                         Serial-Num
--- ---  --------------------------------------  ----------
100 1    000d.ecb1.ef00 to 000d.ecb1.ef2f        JAF1302ABDP
150 1    000d.ecfc.a140 to 000d.ecfc.a16f        JAF1407AARL
151 1    000d.ecf4.f916 to 000d.ecf4.f945        JAF1352AHAL
170 1    68ef.bd62.1080 to 68ef.bd62.109f        JAF1417BTEM
171 1    68ef.bd62.1680 to 68ef.bd62.169f        JAF1421DMEA
198 1    000d.ecf7.d4a3 to 000d.ecf7.d4c2        JAF1352AQCH
199 1    68ef.bd61.d8c0 to 68ef.bd61.d8df        JAF1409ATAM
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show hardware internal	Displays information about the physical hardware.
show inventory	Displays hardware inventory information.

Send comments to nx5000-docfeedback@cisco.com

show processes

To display the process information for the switch, use the **show processes** command.

show processes [**vdc** *vdc-number*]

Syntax Description

vdc *vdc-number*	(Optional) Displays process information for a specific virtual device context (VDC). There is only one VDC on a Cisco Nexus 5000 Series switch.

Command Default

Displays information for all processes running on the switch.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the process information for a device:

```
switch# show processes

PID    State  PC        Start_cnt    TTY   Process
-----  -----  --------  -----------  ----  -------------
    1      S  b7f9e468            1     -  init
    2      S         0            1     -  ksoftirqd/0
    3      S         0            1     -  desched/0
    4      S         0            1     -  events/0
    5      S         0            1     -  khelper
   10      S         0            1     -  kthread
   18      S         0            1     -  kacpid
  169      S         0            1     -  kblockd/0
  182      S         0            1     -  khubd
  247      S         0            1     -  pdflush
  248      S         0            1     -  pdflush
  249      S         0            1     -  kswapd0
  250      S         0            1     -  aio/0
  251      S         0            1     -  SerrLogKthread
  809      S         0            1     -  kide/0
  812      S         0            1     -  ata/0
  817      S         0            1     -  mtdblockd
  845      S         0            1     -  scsi_eh_0
  846      S         0            1     -  usb-storage
 1362      S         0            1     -  kjournald
 1370      S         0            1     -  kjournald
 2127      S         0            1     -  jffs2_gcd_mtd2
 2184      S         0            1     -  kjournald
 2644      S  b7f8718e            1     -  portmap
 2653      S         0            1     -  nfsd
 2654      S         0            1     -  nfsd
 2655      S         0            1     -  nfsd
 2656      S         0            1     -  nfsd
```

Send comments to nx5000-docfeedback@cisco.com

```
 2657      S         0            1     -  nfsd
 2658      S         0            1     -  nfsd
 2659      S         0            1     -  nfsd
 2660      S         0            1     -  nfsd
 2661      S         0            1     -  lockd
 2662      S         0            1     -  rpciod
 2667      S  b7f89468            1     -  rpc.mountd
 2673      S  b7f89468            1     -  rpc.statd
 2700      S  b7df3468            1     -  sysmgr
 3344      S         0            1     -  mping-thread
 3511      S         0            1     -  insmod
 3892      S  b7f4b468            1     -  xinetd
 3893      S  b7f89468            1     -  tftpd
--More--
switch#
```

Related Commands

Command	Description
show processes cpu	Displays the CPU utilization information for processes.
show processes log	Displays the contents of the process log.
show processes memory	Displays the memory allocation information for processes.

Send comments to nx5000-docfeedback@cisco.com

show processes cpu

To display the CPU utilization information for processes on the device, use the **show processes cpu** command.

show processes cpu

Syntax Description

This command has no arguments or keywords.

Command Default

Displays information for all processes in the local device.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the CPU utilization information for the processes:

```
switch# show processes cpu

PID    Runtime(ms)  Invoked   uSecs  1Sec    Process
-----  -----------  --------  -----  ------  -----------
    1         1802     22973     78    0.0%  init
    2          440     44555      9    0.0%  ksoftirqd/0
    3           79     17021      4    0.0%  desched/0
    4         2097     92976     22    0.0%  events/0
    5           71      3224     22    0.0%  khelper
   10            0        18     20    0.0%  kthread
   18            0         2      2    0.0%  kacpid
  169            5       669      8    0.0%  kblockd/0
  182          121        42   2885    0.0%  khubd
  247            0         2      1    0.0%  pdflush
  248          326     20427     15    0.0%  pdflush
  249            0         1      4    0.0%  kswapd0
  250            0         2      1    0.0%  aio/0
  251            0         1      1    0.0%  SerrLogKthread
  809            0         2      1    0.0%  kide/0
  812            0         2      1    0.0%  ata/0
  817            0         1      3    0.0%  mtdblockd
  845            0         1      6    0.0%  scsi_eh_0
  846          132     36789      3    0.0%  usb-storage
 1362            0         1      8    0.0%  kjournald
 1370            0         1      5    0.0%  kjournald
 2127          367        56   6560    0.0%  jffs2_gcd_mtd2
 2184           20       743     27    0.0%  kjournald
 2644            0        21     38    0.0%  portmap
 2653            0        42     14    0.0%  nfsd
 2654            0        30      2    0.0%  nfsd
 2655            0        30      2    0.0%  nfsd
 2656            0        30      2    0.0%  nfsd
 2657            0        30      2    0.0%  nfsd
```

Send comments to nx5000-docfeedback@cisco.com

```
 2658            0        30      2    0.0%  nfsd
 2659            0        32      4    0.0%  nfsd
 2660            0        32      3    0.0%  nfsd
 2661            0         2     33    0.0%  lockd
 2662            0         1      6    0.0%  rpciod
 2667            0         1     71    0.0%  rpc.mountd
 2673            2         5    571    0.0%  rpc.statd
 2700          152    251559      0    0.0%  sysmgr
 3344            0         1     22    0.0%  mping-thread
 3511         1825     10196    179    0.0%  insmod
 3892           12         3   4105    0.0%  xinetd
 3893            3         4    843    0.0%  tftpd
--More--
switch#
```

Related Commands

Command	Description
show processes	Displays the process information for the switch.
show processes log	Displays the contents of the process log.
show processes memory	Displays the memory allocation information for processes.

Send comments to nx5000-docfeedback@cisco.com

show processes log

To display the contents of the process log, use the **show processes log** command.

show processes log [**details** | **pid** *process-id*]

Syntax Description

details	(Optional) Displays detailed information from the process log.
pid *process-id*	(Optional) Displays detailed information from the process log for a specific process. The process ID range is from 1 to 2147483647.

Command Default

Displays summary information for all processes on the device.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display summary information from the process log:

```
switch# show processes log
Process          PID     Normal-exit  Stack  Core   Log-create-time
---------------  ------  -----------  -----  -----  ---------------
afm              2948              N      Y      N  Fri Dec  4 00:36:19 2009
afm              2997              N      Y      N  Tue Dec 15 04:09:57 2009
afm              3871              N      N      N  Sat Mar 20 18:22:14 2010
afm              3875              N      N      N  Fri Mar 26 08:45:06 2010
afm              3877              N      Y      N  Mon Mar 22 03:56:38 2010
afm              3886              N      N      N  Fri Mar 26 08:45:06 2010
afm              3887              N      N      N  Sat Mar 20 18:22:15 2010
afm              3889              N      N      N  Sun Mar 21 06:15:00 2010
afm              3890              N      N      N  Sat Mar 20 18:22:16 2010
afm              3895              N      N      N  Fri Mar 26 08:45:08 2010
afm              3898              N      N      N  Fri Mar 26 08:45:08 2010
afm              3904              N      Y      N  Mon Apr  5 19:28:56 2010
afm              3915              N      N      N  Sun Mar 21 06:15:01 2010
afm              3918              N      Y      N  Mon Mar 22 03:43:42 2010
afm              3919              N      N      N  Sun Mar 21 06:15:03 2010
afm              3922              N      Y      N  Mon Mar 22 03:56:44 2010
afm              3930              N      N      N  Sun Mar 21 06:15:03 2010
afm              3942              N      Y      N  Wed Apr  7 18:47:39 2010
afm              3943              N      Y      N  Tue Apr  6 00:09:46 2010
afm              3950              N      Y      N  Mon Mar 22 03:43:45 2010
afm              3962              N      Y      N  Mon Mar 22 03:43:47 2010
afm              3967              N      Y      N  Tue Apr  6 21:57:55 2010
afm              4054              N      Y      N  Tue Mar 23 07:30:21 2010
afm              4220              N      N      N  Fri Mar 26 08:45:34 2010
afm              4224              N      N      N  Sat Mar 20 18:22:45 2010
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display detailed information from the process log:

```
switch# show processes log details
================================================
Service: afm
Description: Acl manager Daemon

Started at Fri Dec  4 00:36:05 2009 (209115 us)
Stopped at Fri Dec  4 00:36:19 2009 (274038 us)
Uptime: 14 seconds

Start type: SRV_OPTION_RESTART_STATEFUL (24)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Last heartbeat 0.00 secs ago
RLIMIT_AS: 272490099
System image name: n5000-uk9.4.2.1.N1.0.173.bin
System image version: 4.2(1)N1(0.173) S0

PID: 2948
Exit code: signal 11 (core dumped)

CWD: /var/sysmgr/work

Virtual Memory:

    CODE      08048000 - 081467A4
    DATA      08147000 - 0816A968
    BRK       08192000 - 085E3000
    STACK     BFFFFA90
    TOTAL     99840 KB

Register Set:

    EBX B6FA2178         ECX 00000001         EDX 0836EF98
    ESI 0000000C         EDI 0836F040         EBP BFFFEB48
    EAX BFFFEB70         XDS C010007B         XES 0000007B
    EAX FFFFFFFF (orig)  EIP 00000000         XCS 00000073
    EFL 00010296         ESP BFFFEB1C         XSS 0000007B

Stack: 3956 bytes. ESP BFFFEB1C, TOP BFFFFA90

0xBFFFEB1C: B6F3B1EA BFFFEB70 B6568860 00000001 ....p...`.V.....
0xBFFFEB2C: B6F3B1CE 00000000 B6FA2294 0000024F .........."..O...
0xBFFFEB3C: 00000007 0000000C 00000000 BFFFEBD8 ................
0xBFFFEB4C: 08107B82 0836F040 BFFFEB70 BFFFEB68 .{..@.6.p...h...
0xBFFFEB5C: BFFFEB6C B6F71C64 00000000 BFFFEB88 l...d...........
0xBFFFEB6C: B6F4F72A 00000000 00000008 B6F75D71 *...........q]..
--More--
switch#
```

This example shows how to display detailed information from the process log for a specific process:

```
switch# show processes log pid 2948
================================================
Service: afm
Description: Acl manager Daemon

Started at Fri Dec  4 00:36:05 2009 (209115 us)
Stopped at Fri Dec  4 00:36:19 2009 (274038 us)
Uptime: 14 seconds

Start type: SRV_OPTION_RESTART_STATEFUL (24)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Last heartbeat 0.00 secs ago
```

Send comments to nx5000-docfeedback@cisco.com

```
RLIMIT_AS: 272490099
System image name: n5000-uk9.4.2.1.N1.0.173.bin
System image version: 4.2(1)N1(0.173) S0

PID: 2948
Exit code: signal 11 (core dumped)

CWD: /var/sysmgr/work

Virtual Memory:

    CODE      08048000 - 081467A4
    DATA      08147000 - 0816A968
    BRK       08192000 - 085E3000
    STACK     BFFFFA90
    TOTAL     99840 KB

Register Set:

    EBX B6FA2178         ECX 00000001         EDX 0836EF98
    ESI 0000000C         EDI 0836F040         EBP BFFFEB48
    EAX BFFFEB70         XDS C010007B         XES 0000007B
    EAX FFFFFFFF (orig)  EIP 00000000         XCS 00000073
    EFL 00010296         ESP BFFFEB1C         XSS 0000007B

Stack: 3956 bytes. ESP BFFFEB1C, TOP BFFFFA90

0xBFFFEB1C: B6F3B1EA BFFFEB70 B6568860 00000001 ....p...`.V.....
0xBFFFEB2C: B6F3B1CE 00000000 B6FA2294 0000024F .........."..O...
0xBFFFEB3C: 00000007 0000000C 00000000 BFFFEBD8 ................
0xBFFFEB4C: 08107B82 0836F040 BFFFEB70 BFFFEB68 .{..@.6.p...h...
0xBFFFEB5C: BFFFEB6C B6F71C64 00000000 BFFFEB88 l...d...........
0xBFFFEB6C: B6F4F72A 00000000 00000008 B6F75D71 *...........q]..
--More--
switch#
```

Related Commands

Command	Description
show processes	Displays the process information for the switch.
show processes cpu	Displays the CPU utilization information for processes.
show processes memory	Displays the memory allocation information for processes.

Send comments to nx5000-docfeedback@cisco.com

show processes memory

To display the memory allocation information for processes, use the **show processes memory** command.

show processes memory [**shared** [**detail**]]

Syntax Description

shared	(Optional) Displays the shared memory allocation.
detail	(Optional) Displays the shared memory in bytes instead of the default kilobytes.

Command Default

Displays memory allocated to the processes.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information about the memory allocation for processes:

```
switch# show processes memory

PID    MemAlloc StkSize   RSSMem   LibMem    StackBase/Ptr      Process
----   -------  -------  -------   -------   -------------     ---------
    1    147456    86016   495616  1126400 bffffea0/bffff990  init
    2         0        0        0        0        0/0         ksoftirqd/0
    3         0        0        0        0        0/0         desched/0
    4         0        0        0        0        0/0         events/0
    5         0        0        0        0        0/0         khelper
   10         0        0        0        0        0/0         kthread
   18         0        0        0        0        0/0         kacpid
  169         0        0        0        0        0/0         kblockd/0
  182         0        0        0        0        0/0         khubd
  247         0        0        0        0        0/0         pdflush
  248         0        0        0        0        0/0         pdflush
  249         0        0        0        0        0/0         kswapd0
  250         0        0        0        0        0/0         aio/0
  251         0        0        0        0        0/0         SerrLogKthread
  809         0        0        0        0        0/0         kide/0
  812         0        0        0        0        0/0         ata/0
  817         0        0        0        0        0/0         mtdblockd
  845         0        0        0        0        0/0         scsi_eh_0
  846         0        0        0        0        0/0         usb-storage
 1362         0        0        0        0        0/0         kjournald
 1370         0        0        0        0        0/0         kjournald
 2127         0        0        0        0        0/0         jffs2_gcd_mtd2
 2184         0        0        0        0        0/0         kjournald
 2644    155648    86016   438272  1216512 bffffdf0/bffffcf0  portmap
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display information about the shared memory allocation for processes:

```
switch# show processes memory shared
Component             Shared Memory       Size        Used  Available  Reference
                             Address   (kbytes)    (kbytes)   (kbytes)      Count
smm                     0X60000000       1024           3       1021         21
cli                     0X60110000      30720*      13982      16738          6
npacl                   0X61F20000       4096*          1       4095          1
u6rib-ufdm              0X62330000        320*        188        132          1
am                      0X62390000       1024*         13       1011          4
urib                    0X624A0000      32768*        700      32068         11
urib-redist             0X644B0000       4096*          0       4096         11
icmpv6                  0X648C0000       1024           0       1024          1
u6rib                   0X649D0000      16384*        665      15719          5
urib-ufdm               0X659E0000       2048*          0       2048          1
ip                      0X65BF0000       2048          68       1980         10
u6rib-notify            0X65E00000       2048*        795       1253          5
ipv6                    0X66010000       1024          59        965          3
igmp                    0X66120000       1024           0       1024          1
Shared memory totals - Size: 98 MB, Used: 17 MB, Available: 82 MB
switch#
```

Related Commands

Command	Description
show processes	Displays the process information for the switch.
show processes cpu	Displays the CPU utilization information for processes.
show processes log	Displays the contents of the process log.

Send comments to nx5000-docfeedback@cisco.com

show running-config

To display the running configuration, use the **show running-config** command.

show running-config [**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
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display the changes that you have made to the running configuration:

```
switch# show running-config

!Command: show running-config
!Time: Tue Jul 13 06:05:42 2010

version 4.2(1)N2(1)
feature fcoe
feature telnet
feature tacacs+
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex
snmp-server enable traps entity fru
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit command feature environment
  rule 4 permit command feature hardware
  rule 3 permit command feature module
  rule 2 permit command feature snmp
  rule 1 permit command feature system
role name praveena
username admin password 5 $1$VrQsB2KX$4jkUcx3sXWU8lhI1mlwLa/  role network-admin
username oregon password 5 $1$p3VJ0/BY$Kp22A08NeqCQ0asxUKXq91  role network-oper
ator
no password strength-check
ip domain-lookup
ip host switch 192.168.2.215
ip host BEND-1 192.168.2.215
tacacs-server host 192.168.2.54 key 7 "wawy1234"
aaa group server tacacs+ t1
    server 192.168.2.54
```

Send comments to nx5000-docfeedback@cisco.com

```
    use-vrf management
aaa group server tacacs+ tacacs
radius-server host 192.168.2.5 key 7 "KkwyCet" authentication accounting
aaa group server radius r1
    server 192.168.2.5
    use-vrf management
hostname switch
logging event link-status default
errdisable recovery interval 30
no errdisable detect cause link-flap
errdisable recovery cause pause-rate-limit
--More--
switch#
```

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

```
switch# show running-config all
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config diff	Displays the differences between the running configuration and the startup configuration.
show startup-config	Displays the startup configuration.

Send comments to nx5000-docfeedback@cisco.com

show running-config diff

To display the differences between the running configuration and the startup configuration, use the **show running-config diff** command.

show running-config diff

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Table 1-7 describes the notations used in the command output.

Table 1-7 show running-config diff Notations

Notation	Description
********** *--- line1, line2 ----* **** line1, line2 *****	Indicates ranges of lines where differences occur. The range of lines indicated with asterisks (*) is for the startup configuration and the range indicated with dashes (–) is for the startup configuration.
+ text	Indicates that the line is in the running configuration but is not in the startup configuration.
– text	Indicates that the line is not in the running configuration but it is in the startup configuration.
! text	Indicates that the line exists in both configurations but in different orders.

Examples

This example shows how to display the difference between the running configuration and the startup configuration:

```
switch# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1874,1883 ****
--- 1873,1883 ----
  system cores tftp://192.168.2.5/tftpboot/ vrf management
  vsan database
    vsan 700
  cfs eth distribute
  fcdomain fcid database
```

Send comments to nx5000-docfeedback@cisco.com

```
+   vsan 700 wwn 10:00:00:00:00:15:43:e8 fcid 0x350000 dynamic
    vsan 1 wwn 20:44:00:0d:ec:b0:fc:40 fcid 0x780000 dynamic
    vsan 1 wwn 20:43:00:0d:ec:b0:fc:40 fcid 0x780001 dynamic
    vsan 1 wwn 24:01:00:0d:ec:b0:fc:40 fcid 0x780002 dynamic

  interface Vlan1
***************
*** 2089,2103 ****
--- 2089,2113 ----
    priority-flow-control mode on
    speed 1000
    flowcontrol receive on
    service-policy type qos input 1

+ interface port-channel1932
+   shutdown
+   switchport mode trunk
+   switchport trunk allowed vlan 600
+   spanning-tree bpdufilter enable
+   speed 10000
+
  interface vfc1

  interface vfc199
    bind mac-address 00:00:11:11:22:22
+   fcoe fcf-priority 1
    no shutdown
+ vsan database
+   vsan 700 interface vfc199

  interface fc3/1

  interface fc3/2

--More--
switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config	Displays the differences between the running configuration and the startup configuration.
show startup-config	Displays the startup configuration.

Send comments to nx5000-docfeedback@cisco.com

show sprom

To display the contents of the serial PROM (SPROM) on the switch, use the **show sprom** command.

show sprom {**all** | **backplane** | **fex** {*chassis_ID* {**all** | **backplane** | **powersupply** *ps-num*} | **all**} | **module** *module-number* | **powersupply** *ps-num* | **sup**}

Syntax Description

all	Displays the SPROM contents for all components on the physical device.
backplane	Displays the SPROM contents for the backplane.
fex	Displays information about the attached Fabric Extender units.
chassis_ID	(Optional) Fabric Extender chassis ID. The chassis ID is from 100 to 199.
module *module-number*	Displays the SPROM contents for an I/O module. The module number range is from 1 to 3.
powersupply *ps-num*	Displays the SPROM contents for a power supply. The power supply number is 1 or 2.
sup	Displays the SPROM contents for the active supervisor module.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	This command was modified to provide Fabric Extender support.

Usage Guidelines

The SPROM on the switch contains detailed information about the hardware, including serial, part, and revision numbers. If you need to report a problem with a system component, you can extract serial number information using the **show sprom** command.

Examples

This example shows how to display SPROM information for all components on the physical device:

```
switch# show sprom all
DISPLAY backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x17d7
 EEPROM Size     : 65535
 Block Count     : 4
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-C5020P-BF
```

Send comments to nx5000-docfeedback@cisco.com

```
 Serial Number   : SSI13390FZT
 Part Number     : 68-3301-06
 Part Revision   : A0
 Mfg Deviation   : 0
 H/W Version     : 0.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.12.3.1.3.719.0.0
 Power Consump   : 0
 RMA Code        : 0-0-0-0
 CLEI Code       : COMXG00ARC
 VID             : V04
Chassis specific block:
 Block Signature : 0x6001
 Block Version   : 3
 Block Length    : 39
 Block Checksum  : 0x3ca
 Feature Bits    : 0x0
 HW Changes Bits : 0x0
 Stackmib OID    : 0
 MAC Addresses   : 00-0d-ec-e7-df-40
 Number of MACs  : 64
 OEM Enterprise  : 0
 OEM MIB Offset  : 0
 MAX Connector Power: 0
WWN software-module specific block:
 Block Signature : 0x6005
 Block Version   : 1
 Block Length    : 0
 Block Checksum  : 0x20dd
wwn usage bits:
 00 00 00 00 00 00 00 00
--More--
switch#
```

This example shows how to display SPROM information for the backplane:

```
switch# show sprom backplane
DISPLAY backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x17d7
 EEPROM Size     : 65535
 Block Count     : 4
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-C5020P-BF
 Serial Number   : SSI13390FZT
 Part Number     : 68-3301-06
 Part Revision   : A0
 Mfg Deviation   : 0
 H/W Version     : 0.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.12.3.1.3.719.0.0
 Power Consump   : 0
 RMA Code        : 0-0-0-0
 CLEI Code       : COMXG00ARC
 VID             : V04
Chassis specific block:
 Block Signature : 0x6001
```

Send comments to nx5000-docfeedback@cisco.com

```
 Block Version   : 3
--More--
switch#
```

This example shows how to display SPROM information for an attached Fabric Extender:

```
switch# show sprom fex 101 all
```

Related Commands

Command	Description
show hardware internal	Displays information about the physical hardware.
show inventory	Displays hardware inventory information.

Send comments to nx5000-docfeedback@cisco.com

show startup-config

To display the startup configuration, use the **show startup-config** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the startup configuration:

```
switch# show startup-config

!Command: show startup-config
!Time: Tue Jul 13 06:14:51 2010
!Startup config saved at: Fri Jul  9 23:19:25 2010

version 4.2(1)N2(1)
feature fcoe
feature telnet
feature tacacs+
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex
snmp-server enable traps entity fru
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit command feature environment
  rule 4 permit command feature hardware
  rule 3 permit command feature module
  rule 2 permit command feature snmp
  rule 1 permit command feature system
role name praveena
username admin password 5 $1$VrQsB2KX$4jkUcx3sXWU8lhI1mlwLa/  role network-admin
username oregon password 5 $1$p3VJ0/BY$Kp22A08NeqCQ0asxUKXq91  role network-oper
ator
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config	Displays the running configuration.
show running-config diff	Displays the differences between the running configuration and the startup configuration.

Send comments to nx5000-docfeedback@cisco.com

show switchname

To display the hostname for the device, use the **show switchname** command.

show switchname

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show hostname** command also displays the switch hostname.

Examples

This example shows how to display the hostname for the switch:

```
switch# show switchname
```

Related Commands

Command	Description
hostname	Configures the hostname for the switch.
show hostname	Displays the hostname.
switchname	Configures the hostname for the switch.

Send comments to nx5000-docfeedback@cisco.com

show system cores

To display the core filename, use the **show system cores** command.

show system cores

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **system cores** command to configure the system core filename.

Examples

This example shows how to display destination information for the system core files:

```
switch# show system cores
Cores are transferred to tftp://192.168.2.5/tftpboot/
switch#
```

Related Commands

Command	Description
system cores	Configures the system core filename.

Send comments to nx5000-docfeedback@cisco.com

show system reset-reason

To display the reset history for the switch, use the **show system reset-reason** command.

show system reset-reason [**fex** *chassis_ID*]

Syntax Description

fex *chassis_ID*	(Optional) Specifies the Fabric Extender chassis ID. The chassis ID is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	This command was modified to provide Fabric Extender support.

Examples

This example shows how to display the reset-reason history for the switch:

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) No time
    Reason: Unknown
    Service:
    Version: 4.2(1)N2(1)

2) No time
    Reason: Unknown
    Service:
    Version: 4.2(1)N2(1)

3) At 543557 usecs after Fri Jul  9 18:20:45 2010
    Reason: Reset due to upgrade
    Service:
    Version: 4.2(1)N1(1)

4) At 572283 usecs after Fri Jul  9 05:12:27 2010
    Reason: Reset due to upgrade
    Service:
    Version: 4.2(1)N2(1)

switch#
```

This example shows how to display the reset-reason history for an attached Fabric Extender:

```
switch# show system reset-reason fex 100
----- reset reason for FEX 100 ---

1) At 0 usecs after Unknown time
    Reset Reason: Unknown (0)
```

Send comments to nx5000-docfeedback@cisco.com

```
    Service (Additional Info):
    Image Version: 4.2(1)N2(1)

2) At 0 usecs after Unknown time
    Reset Reason: Unknown (0)
    Service (Additional Info):
    Image Version: 4.2(1)N2(1)

3) At 713709 usecs after Fri Jul  9 18:36:32 2010
    Reset Reason: Reset due to upgrade (88)
    Service (Additional Info): Reset due to upgrade
    Image Version: 4.2(1)N1(1)

4) At 702748 usecs after Fri Jul  9 05:27:06 2010
    Reset Reason: Reset due to upgrade (88)
    Service (Additional Info): Reset due to upgrade
    Image Version: 4.2(1)N2(1)

switch#
```

Send comments to nx5000-docfeedback@cisco.com

show system resources

To display the system resources, use the **show system resources** command.

show system resources

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)N2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the system resources on a switch:

```
switch(config)# show system resources
```

Related Commands

Command	Description
show processes cpu	Displays the CPU utilization information for processes on the device.

Send comments to nx5000-docfeedback@cisco.com

show system uptime

To display the amount of time since the last system restart, use the **show system uptime** command.

show system uptime

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the amount of time since the last system restart:

```
switch# show system uptime
System start time:          Mon Jul 12 01:37:08 2010
System uptime:              1 days, 4 hours, 42 minutes, 19 seconds
Kernel uptime:              1 days, 4 hours, 44 minutes, 19 seconds
Active supervisor uptime:   1 days, 4 hours, 42 minutes, 19 seconds
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show tech-support

To display information for Cisco technical support, use the **show tech-support** command.

show tech-support [**brief** | **commands** | *feature*]

Syntax Description

brief	(Optional) Displays information only about the status of the device.
commands	(Optional) Displays the complete list of commands that are executed by the **show tech-support** command.
feature	(Optional) Specific feature name. Use the command-line interface (CLI) context-sensitive help (for example, **show tech-support ?**) for the list of features.

Command Default

Displays information for all features.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The output from the **show tech-support** command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support** > *filename*) in the local writable storage file system or the remote file system.

You can use one of the following redirection methods:

- > *filename*—Redirects the output to a file.
- >> *filename*—Redirects the output to a file in append mode.

Examples

This example shows how to display technical support information:

```
switch# show tech-support
---- show tech-support ----
`show switchname`
switch
`show system uptime`
System start time:          Mon Jul 12 01:37:08 2010
System uptime:              1 days, 4 hours, 42 minutes, 53 seconds
Kernel uptime:              1 days, 4 hours, 44 minutes, 54 seconds
Active supervisor uptime:   1 days, 4 hours, 42 minutes, 53 seconds
`show interface mgmt0`
mgmt0 is up
  Hardware: GigabitEthernet, address: 000d.ece7.df40 (bia 000d.ece7.df40)
  Internet Address is 192.168.1.215/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Send comments to nx5000-docfeedback@cisco.com

```
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  1 minute input rate 5408 bits/sec, 4 packets/sec
  1 minute output rate 1320 bits/sec, 1 packets/sec
  Rx
    465934 input packets 311703 unicast packets 73820 multicast packets
    80411 broadcast packets 250277048 bytes
  Tx
    158490 output packets 155374 unicast packets 1725 multicast packets
    1391 broadcast packets 13184030 bytes

`show system resources`
Load average:   1 minute: 2.28   5 minutes: 1.77   15 minutes: 1.30
--More--
switch#
```

This example shows how to redirect the technical support information to a file:

```
switch# show tech-support > bootflash:TechSupport.txt
```

This example shows how to display the brief technical support information for the switch:

```
switch# show tech-support brief
Switch Name           : switch
Switch Type           : 40x10GE/Supervisor
Kickstart Image       : 4.2(1)N2(1) bootflash:/sanity-kickstart
System Image          : 4.2(1)N2(1) bootflash:/sanity-system
IP Address/Mask       : 192.168.1.215/24
No of VSANs           : 2
Configured VSANs      : 1,700

VSAN    1:    name:VSAN0001, state:active, interop mode:default
              domain id:0x78(120), WWN:20:01:00:0d:ec:e7:df:41 [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN  700:    name:VSAN0700, state:active, interop mode:default
              domain id:0x35(53), WWN:22:bc:00:0d:ec:e7:df:41 [Principal]
              active-zone:<NONE>, default-zone:permit


--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc3/1      1      auto   on      sfpAbsent        --     --           --
fc3/2      1      auto   on      sfpAbsent        --     --           --
fc3/3      1      auto   on      down             swl    --           --
fc3/4      1      auto   on      down             swl    --           --
fc3/5      1      auto   on      sfpAbsent        --     --           --
--More--
switch#
```

This example shows how to display the technical support information for a specific feature:

```
switch# show tech-support aaa
`show running-config aaa all`

!Command: show running-config aaa all
!Time: Tue Jul 13 06:23:49 2010

version 4.2(1)N2(1)
aaa authentication login default local
aaa authorization config-commands default local
aaa authorization commands default local
```

Send comments to nx5000-docfeedback@cisco.com

```
aaa accounting default local
aaa user default-role
no aaa authentication login error-enable
no aaa authentication login mschap enable
no aaa authentication login mschapv2 enable
no aaa authentication login ascii-authentication
no radius-server directed-request
no tacacs-server directed-request


`show system internal aaa event-history msgs`
1) Event:E_MTS_RX, length:60, at 932934 usecs after Tue Jul 13 06:23:49 2010
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X011968A2, Ret:SUCCESS
    Src:0x00000101/7389, Dst:0x00000101/111, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x011968A2, Sync:UNKNOWN, Payloadsize:216
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 31 39

--More--
switch#
```

This example shows how to display the commands used to generate the technical support information:

```
switch# show tech-support commands
```

Send comments to nx5000-docfeedback@cisco.com

show terminal

To display information about the terminal configuration for a session, use the **show terminal** command.

show terminal

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information about the terminal configuration for a session:

```
switch# show terminal
TTY: /dev/pts/1 Type: "ansi"
Length: 29 lines, Width: 80 columns
Session Timeout: 0 minutes
Event Manager CLI event bypass: no
Redirection mode: ascii
switch#
```

Related Commands

Command	Description
terminal length	Configures the terminal display length for the session.
terminal session-timeout	Configures the terminal inactive session timeout for a session.
terminal type	Configures the terminal type for a session.
terminal width	Configures the terminal display width for a session.

Send comments to nx5000-docfeedback@cisco.com

show version

To display information about the software version, use the **show version** command.

show version [**fex** *chassis_ID* | **image** *filename*]

Syntax Description

fex *chassis_ID*	(Optional) Specifies the Fabric Extender chassis ID. The chassis ID is from 100 to 199.
image *filename*	(Optional) Displays the version information for a system or kickstart image file.

Command Default

Displays software version information for the running kickstart and system images.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	This command was modified to provide Fabric Extender support.

Examples

This example shows how to display the version information for the kickstart and system image running on the device:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2010, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.3.0
  loader:    version N/A
  kickstart: version 4.2(1)N2(1)
  system:    version 4.2(1)N2(1)
  power-seq: version v1.2
  BIOS compile time:       09/08/09
  kickstart image file is: bootflash:/sanity-kickstart
  kickstart compile time:  7/28/2010 11:00:00 [07/07/2010 22:20:39]
  system image file is:    bootflash:/sanity-system
  system compile time:     7/28/2010 11:00:00 [07/07/2010 23:47:55]


Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Xeon(R) CPU         with 2074288 kB of memory.
  Processor Board ID JAF1344BHNK
```

Send comments to nx5000-docfeedback@cisco.com

```
  Device name: NEXUS5K-1
  bootflash:    1003520 kB

Kernel uptime is 0 day(s), 9 hour(s), 9 minute(s), 7 second(s)

Last reset
  Reason: Unknown
  System version: 4.2(1)N2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin, Fc Plugin
switch#
```

This example shows how to display the version information for an attached Fabric Extender:

```
switch# show version fex 100
Software
  Bootloader version:           1.12
  System boot mode:             primary
  System image version:         4.2(1)N2(1) [build 4.2(1)N2(1)]

Hardware
  Module:                       Fabric Extender 48x1GE Module
  CPU:                          Motorola, e300c1
  Serial number:                JAF1302ABDP
  Bootflash:                    locked

Kernel uptime is 0 day(s), 9 hour(s), 9 minutes(s), 16 second(s)

Last reset at Fri Jul 02 04:27:04 2010
  Reason: Reset Requested by CLI command reload
  Service: Reload requested by supervisor
switch#
```

Send comments to nx5000-docfeedback@cisco.com

sleep

To cause the command-line interface (CLI) to pause before displaying the prompt, use the **sleep** command.

sleep *seconds*

Syntax Description

seconds	Number of seconds. The range is from 0 to 2147483647.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can use this command in command scripts to delay the execution of the script.

Examples

This example shows how to cause the CLI to pause for 5 seconds before displaying the prompt:

```
switch# sleep 5
```

Related Commands

Command	Description
run-script	Runs command scripts.

Send comments to nx5000-docfeedback@cisco.com

speed

To configure the transmit and receive speed for the console port, use the **speed** command. To revert to the default, use the **no** form of this command.

speed *speed*

no speed *speed*

Syntax Description

speed	Speed in bits per second. Valid speeds are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.

Command Default

The default console port speed is 9600 bits per second.

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the speed for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# speed 57600
```

This example shows how to revert to the default speed for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no speed 57600
```

Related Commands

Command	Description
line console	Enters the console terminal configuration mode.
show running-config	Displays the running configuration.

Send comments to nx5000-docfeedback@cisco.com

stopbits

To configure the stop bits for the console port, use the **stopbits** command. To revert to the default, use the **no** form of this command.

stopbits {**1** | **2**}

no stopbits {**1** | **2**}

Syntax Description

1	Specifies one stop bit.
2	Specifies two stop bits.

Command Default

1 stop bit

Command Modes

Terminal line configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the number of stop bits for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# stopbits 2
```

This example shows how to revert to the default number of stop bits for the console port:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# no stopbits 2
```

Related Commands

Command	Description
line console	Enters the console terminal configuration mode.
show running-config	Displays the running configuration.

Send comments to nx5000-docfeedback@cisco.com

switchname

To configure the hostname for the device, use the **switchname** command. To revert to the default, use the **no** form of this command.

switchname *name*

no switchname

Syntax Description

name	Hostname for the switch. The name is alphanumeric, case sensitive, can contain special characters, and can have a maximum of 32 characters.

Command Default

"switch" is the default hostname.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software uses the hostname in command-line interface (CLI) prompts and in default configuration filenames.

The **switchname** command performs the same function as the **hostname** command.

Examples

This example shows how to configure the hostname for a Cisco Nexus 5000 Series switch:

```
switch# configure terminal
switch(config)# switchname Engineering2
Engineering2(config)#
```

This example shows how to revert to the default hostname:

```
Engineering2# configure terminal
Engineering2(config)# no switchname
switch(config)#
```

Related Commands

Command	Description
hostname	Configures the switch hostname.
show hostname	Displays the switch hostname.
show switchname	Displays the switch hostname.

Send comments to nx5000-docfeedback@cisco.com

system cores

To configure the destination for the system core, use the **system cores** command. To revert to the default, use the **no** form of this command.

system cores tftp:*tftp_URL* [**vrf management**]

no system cores

Syntax Description

tftp:	Specifies a TFTP server.
tftp_URL	URL for the destination file system and file. Use the following format: [//*server*[:*port*]][/*path*/]*filename*
vrf management	(Optional) Specifies to use the management virtual routing and forwarding (VRF).

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure a core file:

```
switch# configure terminal
switch(config)# system cores tftp://serverA:69/core_file
```

This example shows how to disable system core logging:

```
switch# configure terminal
switch(config)# no system cores
```

Related Commands

Command	Description
show system cores	Displays the core filename.

Send comments to nx5000-docfeedback@cisco.com

system startup-config unlock

To unlock the startup configuration file, use the **system startup-config unlock** command.

system startup-config unlock *process-id*

Syntax Description

process-id	Identifier of the process that has locked the startup-configuration file.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **show system internal sysmgr startup-config locks** command to display the locks on the startup configuration file.

Examples

This example shows how to unlock the startup-configuration file:

```
switch# system startup-config unlock 10
```

Send comments to nx5000-docfeedback@cisco.com

tail

To display the last lines of a file, use the **tail** command.

tail [*filesystem***:** [*//server/*]] [*directory*] *filename* [*lines*]

Syntax Description

*filesystem***:**	(Optional) Name of the file system. Valid values are **bootflash**, **modflash**, or **volatile**.
//server/	(Optional) Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
filename	Name of the file to display. The filename is case sensitive.
lines	(Optional) Number of lines to display. The range is from 0 to 80.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

Displays the last 10 lines.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the last 10 lines of a file:

```
switch# tail bootflash:startup.cfg
```

This example shows how to display the last 20 lines of a file:

```
switch# tail bootflash:startup.cfg 20
```

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Copies files.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

Send comments to nx5000-docfeedback@cisco.com

terminal length

To set the number of lines of output to display on the terminal screen for the current session before pausing, use the **terminal length** command. To revert to the default, use the **no** form of this command.

terminal length *lines*

terminal no length

Syntax Description

lines	Number of lines to display. The range is from 0 to 511. Use 0 to not pause while displaying output.

Command Default

The initial default for the console is 0 (do not pause output). The initial default for virtual terminal sessions is defined by the client software. The default for the **no** form is 24 lines.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The session pauses after displaying the number of lines set in the terminal length. Press the space bar to display another screen of lines or press the **Enter** key to display another line. To return to the command prompt, press **Ctrl-C**.

The terminal length setting applies only to the current session.

Examples

This example shows how to set the number of lines of command output to display on the terminal before pausing:

```
switch# terminal length 28
```

This example shows how to revert to the default number of lines:

```
switch# terminal no length
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

Send comments to nx5000-docfeedback@cisco.com

terminal session-timeout

To set the terminal inactivity timeout for the current session, use the **terminal session-timeout** command. To revert to the default, use the **no** form of this command.

terminal session-timeout *minutes*

terminal no session-timeout

Syntax Description

minutes	Number of minutes. The range is from 0 to 525600 minutes (8760 hours). Use 0 to disable the terminal inactivity timeout.

Command Default

Terminal session timeout is disabled (0 minutes).

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The terminal session inactivity timeout setting applies only to the current session.

Examples

This example shows how to set the terminal inactivity timeout for the session to 10 minutes:

```
switch# terminal session-timeout 10
```

This example shows how to revert to the default terminal inactivity timeout for the session:

```
switch# terminal no session-timeout
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

Send comments to nx5000-docfeedback@cisco.com

terminal terminal-type

To set the terminal type for the current session, use the **terminal terminal-type** command. To revert to the default, use the **no** form of this command.

terminal terminal-type *type*

terminal no terminal-type

Syntax Description

type	Type of terminal. The type string is case sensitive, must be a valid type (for example, ansi, vt100, or xterm), and has a maximum of 80 characters.

Command Default

For a virtual terminal, the terminal type is set during negotiation with the client software. Otherwise, vt100 is the default.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The terminal type setting applies only to the current session.

Examples

This example shows how to set the terminal type:

```
switch# terminal terminal-type xterm
```

This example shows how to revert to the default terminal type:

```
switch# terminal no terminal-type
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

Send comments to nx5000-docfeedback@cisco.com

terminal width

To set the number of character columns on the terminal screen for the current line for a session, use the **terminal width** command. To revert to the default, use the **no** form of this command.

terminal width *columns*

terminal no width

Syntax Description

columns	Number of columns. The range is from 24 to 511.

Command Default

For a virtual terminal, the width is set during negotiation with the client software. Otherwise, 80 columns is the default.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The terminal width setting applies only to the current session.

Examples

This example shows how to set the number of columns to display on the terminal:

```
switch# terminal width 70
```

This example shows how to revert to the default number of columns:

```
switch# terminal no width
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

Send comments to nx5000-docfeedback@cisco.com

traceroute

To discover the routes that packets take when traveling to an IP address, use the **traceroute** command.

traceroute {*dest-addr* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}] [**source** *src-addr*]

Syntax Description

dest-addr	IP address of the destination device. The format is *A.B.C.D*.
hostname	Name of the destination device. The name is case sensitive.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.
source *src-addr*	(Optional) Specifies a source IP address. The format is *A.B.C.D*. The default is the IPv4 address for the management interface of the switch.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to discover a route to a network device:

```
switch# traceroute 192.168.255.18 vrf management
```

Related Commands

Command	Description
ping	Displays the network connectivity to another network device.
traceroute6	Discovers the route to a device using IPv6 addressing.

Send comments to nx5000-docfeedback@cisco.com

traceroute6

To discover the routes that packets take when traveling to an IPv6 address, use the **traceroute6** command.

traceroute6 {*dest-addr* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}] [**source** *src-addr*]

Syntax Description

dest-addr	IPv6 address of the destination device. The format is *A*:*B*::*C*:*D*.
hostname	Name of the destination device. The name is case sensitive.
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	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.
source *src-addr*	(Optional) Specifies a source IPv6 address. The format is *A*:*B*::*C*:*D*. The default is the IPv6 address for the management interface of the switch.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Examples

This example shows how to discover a route to a device:

```
switch# traceroute6 2001:0DB8::200C:417A vrf management
```

Related Commands

Command	Description
ping6	Determines connectivity to another device using IPv6 addressing.
traceroute	Discovers the route to a device using IPv4 addressing.

Send comments to nx5000-docfeedback@cisco.com

update license

To update an existing license, use the **update license** command.

update license [*filesystem***:** [//*server*/]] [*directory*] *src-filename* [*target-filename*]

Syntax Description

*filesystem***:**	(Optional) Name of the file system. Valid values are **bootflash** or **volatile**.
//*server*/	(Optional) Name of the server. Valid values are ///, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory	(Optional) Name of a directory. The directory name is case sensitive.
src-filename	Name of the source license file.
target-filename	(Optional) Name of the target license file.

Note There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to update a license:

```
switch# update license bootflash:fm.lic fm-update.lic
```

Related Commands

Command	Description
show license	Displays license information.

Send comments to nx5000-docfeedback@cisco.com

write erase

To erase configurations in persistent memory areas, use the **write erase** command.

write erase [**boot** | **debug**]

Syntax Description

boot	(Optional) Erases only the boot configuration.
debug	(Optional) Erases only the debug configuration.

Command Default

Erases all configuration in persistent memory.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can use this command to erase the startup configuration in the persistent memory when information is corrupted or otherwise unusable. Erasing the startup configuration returns the switch to its initial state.

Examples

This example shows how to erase the startup configuration:

```
switch# write erase
```

This example shows how to erase the debug configuration in the persistent memory:

```
switch# write erase debug
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config	Displays the startup configuration.

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 2

Ethernet Commands

This chapter describes the Cisco NX-OS Ethernet commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

bandwidth (interface)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command. To restore the default values, use the **no** form of this command.

bandwidth {*kbps* | **inherit** [*kbps*]}

no bandwidth {*kbps* | **inherit** [*kbps*]}

Syntax Description

kbps	Informational bandwidth in kilobits per second. Valid values are from 1 to 10000000.
inherit	(Optional) Specifies the bandwidth inherited from the main interface.

Command Default

1000000 kbps

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If a bandwidth is not configured on a subinterface, and you use the **bandwidth inherit** command, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the bandwidth inherit command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an interface has an explicit bandwidth setting configured, then that interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

Examples

This example shows how to configure all subinterfaces off this main interface to inherit the configured bandwidth:

```
switch(config-if)# bandwidth inherit 30000
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send comments to nx5000-docfeedback@cisco.com

cdp

To enable the Cisco Discovery Protocol (CDP) and configure CDP attributes, use the **cdp** command. To disable CDP or reset CDP attributes, use the **no** form of this command.

cdp {**advertise** {**v1** | **v2**} | **enable** | **format device-id** {**mac-address** | **serial-number** | **system-name**} | **holdtime** *seconds* | **timer** *seconds*}

no cdp {**advertise** | **enable** | **format device-id** {**mac-address** | **serial-number** | **system-name**} | **holdtime** *seconds* | **timer** *seconds*}

Syntax Description

advertise {**v1** | **v2**}	Configures the version to use to send CDP advertisements. Version-2 is the default state.
enable	Enables CDP for all Ethernet interfaces.
format device-id	Configures the format of the CDP device ID.
mac-address	Uses the MAC address as the CDP device ID.
serial-number	Uses the serial number as the CDP device ID.
system-name	Uses the system name, which can be expressed as a fully qualified domain name, as the CDP device ID. This is the default.
holdtime *seconds*	Specifies the amount of time a receiver should hold CDP information before discarding it. The range is from 10 to 255 seconds; the default is 180 seconds.
timer *seconds*	Sets the transmission frequency of CDP updates in seconds. The range is from 5 to 254; the default is 60 seconds.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable CDP on all Ethernet interfaces:

```
switch# configure terminal
switch(config)# cdp enable
```

This example shows how to configure the MAC address as the CDP device ID:

```
switch# configure terminal
switch(config)# cdp format device-id mac-address
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to disable CDP on all Ethernet interfaces:

```
switch# configure terminal
switch(config)# no cdp enable
```

Related Commands

Command	Description
show cdp	Displays Cisco Discovery Protocol (CDP) information.

Send comments to nx5000-docfeedback@cisco.com

cdp enable

To enable the Cisco Discovery Protocol (CDP) on an Ethernet interface, use the **cdp enable** command. To disable CDP on the interface, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable CDP on an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# cdp enable
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send comments to nx5000-docfeedback@cisco.com

channel-group (Ethernet)

To assign and configure a physical interface to an EtherChannel, use the **channel-group** command. To remove the channel group configuration from the interface, use the **no** form of this command.

channel-group *number* [**mode** {**active** | **on** | **passive**}]

no channel-group [*number*]

Syntax Description

number	Number of channel group. The *number* range is from 1 to 4096. Cisco NX-OS creates the EtherChannel associated with this channel group if the EtherChannel does not already exist.
mode	(Optional) Specifies the EtherChannel mode of the interface.
active	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. The interface is in an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
on	This is the default channel mode. Specifies that all EtherChannels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the switch returns an error message. After you enable LACP globally, by using the **feature lacp** command, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the channel group. The default mode is **on**.
passive	Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected. The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Send comments to nx5000-docfeedback@cisco.com

Usage Guidelines

Use this command to create a channel group that includes the interface that you are working on and to add or remove specific interfaces from the channel group. Use this command to move a port from one channel group to another. You enter the channel group that you want the port to move to; the switch automatically removes the specified port from its present channel group and adds it to the specified channel group.

After you enable LACP globally, by using the **feature lacp** command, you enable LACP on each channel by configuring the channel mode as either **active** or **passive**. An EtherChannel in the **on** channel mode is a pure EtherChannel and can aggregate a maximum of eight ports. The EtherChannel does not run LACP.

You cannot change the mode for an existing EtherChannel or any of its interfaces if that EtherChannel is not running LACP; the channel mode remains as **on**. The system returns an error message if you attempt to change the mode.

Use the **no** form of this command to remove the physical interface from the EtherChannel. When you delete the last physical interface from an EtherChannel, the EtherChannel remains. To delete the EtherChannel completely, use the **no** form of the **interface port-channel** command.

The compatibility check includes the following operational attributes:

- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- SPAN (cannot be SPAN source or destination port)
- Storm control

Use the **show port-channel compatibility-parameters** command to see the full list of compatibility checks that Cisco NX-OS uses.

You can only add interfaces configured with the channel mode set to **on** for static EtherChannels, that is, without a configured aggregation protocol. You can only add interfaces configured with the channel mode as **active** or **passive** to EtherChannels that are running LACP.

You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, Cisco NX-OS suspends that port in the EtherChannel.

When the interface joins an EtherChannel, some of its individual parameters are overridden with the values on the EtherChannel, as follows:

- MAC address
- Spanning Tree Protocol (STP)
- Service policy
- Quality of service (QoS)
- Access control lists (ACLs)

Interface parameters, such as the following, remain unaffected when the interface joins or leaves a EtherChannel:

- Description
- Cisco Discovery Protocol (CDP)
- LACP port priority

Send comments to nx5000-docfeedback@cisco.com

- Debounce
- Rate mode
- Shutdown
- SNMP trap

If interfaces are configured for the EtherChannel interface and a member port is removed from the EtherChannel, the configuration of the EtherChannel interface is not propagated to the member ports.

Any configuration changes that you make in any of the compatibility parameters to the EtherChannel interface are propagated to all interfaces within the same channel group as the EtherChannel (for example, configuration changes are also propagated to the physical interfaces that are not part of the EtherChannel but are part of the channel group).

Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 mode active
```

Related Commands

Command	Description
show interface port-channel	Displays information about the traffic on the specified EtherChannel interface.
show lacp	Displays LACP information.
show port-channel summary	Displays information on the EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

clear mac access-list counters

To clear statistical information from the access list, use the **clear mac access-list counters** command.

clear mac access-list counters [*name*]

Syntax Description

name	(Optional) Name of a specific counter to clear.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear statistical information from the access list:

```
switch# clear mac access-list counters
```

Related Commands

Command	Description
show mac access-lists	Displays the information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

clear mac address-table dynamic

To clear the dynamic address entries from the MAC address table, use the **clear mac address-table dynamic** command.

clear mac address-table dynamic [[**address** *mac-addr*] | [**interface** {*type slot*/*port* | **port-channel** *number*}]] [**vlan** *vlan-id*]

Syntax Description

address *mac-addr*	(Optional) Specifies the MAC address to remove from the table. Use the format EEEE.EEEE.EEEE.
interface *type slot*/*port*	(Optional) Specifies the interface for which MAC addresses should be removed from the table. The type can be either Ethernet or EtherChannel. Specify the appropriate slot or virtual interface group number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel for which MAC addresses should be removed from the table. Use the EtherChannel number. The *number* range is from 1 to 4096.
vlan *vlan-id*	(Optional) Specifies the VLAN from which MAC addresses should be removed from the table. The VLAN ID range is from 1 to 4094.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **clear mac address-table dynamic**.

Usage Guidelines

Use the **clear mac address-table dynamic** command with no arguments to remove all dynamic entries from the table.

To clear static MAC addresses from the table, use the **no mac address-table static** command.

If the **clear mac address-table dynamic** command is entered with no options, all dynamic addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, the switch removes all addresses on the specified interfaces.

Examples

This example shows how to clear all the dynamic entries from the MAC address table:

```
switch# clear mac address-table dynamic
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to clear all the dynamic entries from the MAC address table for VLAN 2:

```
switch# clear mac address-table dynamic vlan 2
```

Related Commands

Command	Description
show mac address-table	Displays the information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

clear spanning-tree counters

To clear the counters for the Spanning Tree Protocol (STP), use the **clear spanning-tree counters** command.

clear spanning-tree counters [**interface** {**ethernet** *interface* | **port-channel** *channel*}] [**vlan** *vlan-id*]

Syntax Description

interface	(Optional) Specifies the interface type.
ethernet *interface*	Specifies the slot and port number.
port-channel *channel*	Specifies the EtherChannel number.
vlan *vlan-id*	(Optional) Specifies the VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can clear all the STP counters on the entire switch, per VLAN, or per interface.

Examples

This example shows how to clear the STP counters for VLAN 5:

```
switch# clear spanning-tree counters vlan 5
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

clear spanning-tree detected-protocol

To restart the protocol migration, use the **clear spanning-tree detected-protocol** command. With no arguments, the command is applied to every port of the switch.

clear spanning-tree detected-protocol [**interface** {**ethernet** *interface* | **port-channel** *channel*}]

Syntax Description

interface	(Optional) Specifies the interface type.
ethernet *interface*	Specifies the slot and port number.
port-channel *channel*	Specifies the EtherChannel number.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a switch running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy device. An MST switch can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region.

These mechanisms are not always able to revert to the most efficient mode. For example, a Rapid PVST+ switch that is designated for a legacy 802.1D bridge stays in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port assumes that it is a boundary port when the bridges to which it is connected have joined the same region.

To force a port to renegotiate with its neighbors, enter the **clear spanning-tree detected-protocol** command.

Examples

This example shows how to restart the protocol migration on a specific interface:

```
switch# clear spanning-tree detected-protocol interface ethernet 1/4
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

delay (interface)

To set a delay value for an interface, use the **delay** command. To restore the default delay value, use the **no** form of this command.

delay *tens-of-microseconds*

no delay

Syntax Description

tens-of-microseconds	Throughput delay in tens of microseconds.

Command Default

10 microseconds

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to set a delay of 30,000 microseconds on an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# delay 3000
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send comments to nx5000-docfeedback@cisco.com

description (interface)

To add a description to an interface 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 interface configuration. This string is limited to 80 characters.

Command Default

No description is added.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **description** command is meant to provide a reminder in the configuration to describe what certain interfaces are used for. The description appears in the output of the following commands such as **show interface** and **show running-config**.

Examples

This example shows how to add a description for an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# description "10G Server Link"
```

Related Commands

Command	Description
show interface ethernet	Displays the interface configuration information.
show running-config	Displays the contents of the currently running configuration file.

Send comments to nx5000-docfeedback@cisco.com

errdisable detect cause

To enable error-disable (err-disabled) detection in an application, use the **errdisable detect cause** command. To disable error disable detection, use the **no** form of this command.

errdisable detect cause {all | link-flap | loopback}

no errdisable detect cause {all | link-flap | loopback}

Syntax Description

all	Enables error detection on all cases.
link-flap	Enables error disable detection on linkstate-flapping.
loopback	Enables error disable detection on loopback.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

When error disable detection is enabled and a cause is detected on an interface, the interface is placed in an err-disabled state, which is an operational state that is similar to the link-down state.

Examples

This example shows how to enable the err-disabled detection on linkstate-flapping:

```
switch(config)# errdisable detect cause link-flap
switch(config)#
```

Related Commands

Command	Description
errdisable recovery	Configures recovery from the err-disabled state.
show interface status err-disabled	Displays the interface error disabled state.

Send comments to nx5000-docfeedback@cisco.com

errdisable recovery cause

To configure the application to bring the interface out of the error-disabled (err-disabled) state and retry coming up, use the **errdisable recovery cause** command. To revert to the defaults, use the **no** form of this command.

errdisable recovery cause {**all** | **bpduguard** | **link-flap-recovery** | **failed-port-state** | **pause-rate-limit** | **udld**}

no errdisable recovery cause {**all** | **bpduguard** | **link-flap-recovery** | **failed-port-state** | **pause-rate-limit** | **udld**}

Syntax Description

all	Enables timer to recover from all causes.
bpduguard	Enables timer to recover from bridge protocol data unit (BPDU) Guard error disable state.
failed-port-state	Enables timer to recover from stp set port state failure.
link-flap	Enables timer to recover from linkstate flapping.
pause-rate-limit	Enables timer to recover from pause rate limit error disabled state.
udld	Enables timer to recover from udld error disabled state.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

When error disable recovery is enabled, the interface automatically recovers from the err-disabled state, and the device retries bringing the interface up.

Examples

This example shows how to enable error disable recovery from linkstate-flapping:

```
switch(config)# errdisable recovery cause link-flap
switch(config)#
```

Related Commands

Command	Description
errdisable detect cause	Enables the errror disabled (err-disabled) detection.
show interface status err-disabled	Displays the interface error disabled state.

Send comments to nx5000-docfeedback@cisco.com

errdisable recovery interval

To configure the recovery time interval to bring the interface out of the error-disabled (err-disabled) state, use the **errdisable recovery interval** command. To revert to the defaults, use the **no** form of this command.

errdisable recovery interval *time*

no errdisable recovery interval

Syntax Description

time	Error disable recovery time interval. The range is from 30 to 65535 seconds.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

When error disable recovery is enabled, the interface automatically recovers from the err-disabled state, and the device retries bringing the interface up.

The device waits 300 seconds to retry.

Examples

This example shows how to enable error disable recovery time interval to 100 seconds:

```
switch(config)# errdisable recovery interval 100
switch(config)#
```

Related Commands

Command	Description
errdisable recovery cause	Enables errror disabled recovery on an interface.
show interface status err-disabled	Displays the interface error disabled state.

Send comments to nx5000-docfeedback@cisco.com

feature vtp

To enable VLAN Trunking Protocol (VTP), use the **feature vtp** command. To disable VTP, use the **no** form of this command.

feature vtp

no feature vtp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to enable VTP on the switch:

```
switch(config)# feature vtp
```

Related Commands

Command	Description
show vtp status	Displays the VTP information.
vtp	Configures VTP.

Send comments to nx5000-docfeedback@cisco.com

hardware multicast hw-hash

To use hardware hashing for multicast traffic on an EtherChannel interface, use the **hardware multicast hw-hash** command. To restore the defaults, use the **no** form of this command.

hardware multicast hw-hash

no hardware multicast hw-hash

Syntax Description

This command has no arguments or keywords.

Command Default

The software selection method is used for multicast traffic.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)N2(1)	This command was introduced.

Usage Guidelines

By default, ingress multicast traffic on any port in the switch selects a particular EtherChannel member to egress the traffic. To reduce potential issues with the bandwidth and to provide effective load balancing of the ingress multicast traffic, hardware hashing is used for multicast traffic.

Note Hardware hashing is not available on a Cisco Nexus 2000 Series Fabric Extender HIF port (downlink port).

Examples

This example shows how to set the hardware hashing for multicast traffic on an EtherChannel interface:

```
switch(config)# interface port-channel 21
switch(config-if)# hardware multicast hw-hash
switch(config-if)#
```

This example shows how to restore the default software selection method for multicast traffic on an EtherChannel interface:

```
switch(config)# interface port-channel 21
switch(config-if)# hardware multicast hw-hash
switch(config-if)# no hardware multicast hw-hash
switch(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays the status of the EtherChannel interface configuration.

Send comments to nx5000-docfeedback@cisco.com

instance vlan

To map a VLAN or a set of VLANs to a Multiple Spanning Tree instance (MSTI), use the **instance vlan** command. To delete the instance and return the VLANs to the default instance (Common and Internal Spanning Tree [CIST]), use the **no** form of this command.

instance *instance-id* **vlan** *vlan-id*

no instance *instance-id* [**vlan** *vlan-id*]

Syntax Description

instance-id	Instances to which the specified VLANs are mapped. The range is from 0 to 4094.
vlan *vlan-id*	Specifies the number of the VLANs that you are mapping to the specified MSTI. The VLAN ID range is from 1 to 4094.

Command Default

No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes

MST configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The VLAN identifier is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added to or removed from the existing instances.

Any unmapped VLAN is mapped to the CIST instance.

Caution When you change the VLAN-to-MSTI mapping, the system restarts MST.

Examples

This example shows how to map a range of VLANs to MSTI 4:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 4 vlan 100-200
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree mst configuration	Displays information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration mode.

Send comments to nx5000-docfeedback@cisco.com

interface ethernet

To enter interface configuration mode for an Ethernet IEEE 802.3 interface, use the **interface ethernet** command.

interface ethernet [*chassis_ID*/] *slot*/*port*

Syntax Description

chassis_ID	(Optional) Specifies the Fabric Extender chassis ID. The chassis ID is from 100 to 199. **Note** This argument is not optional when addressing the host interfaces of a Cisco Nexus 2000 Series Fabric Extender.
slot	Slot from 1 to 3. The following list defines the slots available: • Slot 1 includes all the fixed ports. A Fabric Extender only has one slot. • Slot 2 includes the ports on the upper expansion module (if populated). • Slot 3 includes the ports on the lower expansion module (if populated).
port	Port number within a particular slot. The port number is from 1 to 128.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N2(1)	This command was modified to provide the chassis ID argument.

Examples

This example shows how to enter configuration mode for Ethernet interface 1/4:

```
switch(config)# interface ethernet 1/4
switch(config-if)#
```

This example shows how to enter configuration mode for a host interface on a Fabric Extender:

```
switch(config)# interface ethernet 101/1/1
switch(config-if)#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show interface ethernet	Displays various parameters of an Ethernet IEEE 802.3 interface.
speed	Sets the speed on the interface.

Send comments to nx5000-docfeedback@cisco.com

interface port-channel

To create an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command. To remove an EtherChannel interface, use the **no** form of this command.

interface port-channel *channel-number*

no interface port-channel *channel-number*

Syntax Description

channel-number	Channel number that is assigned to this EtherChannel logical interface. The range is from 1 to 4096.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

A port can belong to only one channel group.

When you use the **interface port-channel** command, follow these guidelines:

- If you are using CDP, you must configure it only on the physical interface and not on the EtherChannel interface.
- If you do not assign a static MAC address on the EtherChannel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the EtherChannel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

Examples

This example shows how to create an EtherChannel group interface with channel-group number 50:

```
switch(config)# interface port-channel 50
switch(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays information on traffic about the specified EtherChannel interface.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show lacp	Displays LACP information.
show port-channel summary	Displays information on the EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

ip igmp snooping (EXEC)

To enable Internet Group Management Protocol (IGMP), use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP snooping is enabled.

Note If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable IGMP snooping:

```
switch# ip igmp snooping
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information and configuration.

Send comments to nx5000-docfeedback@cisco.com

ip igmp snooping (VLAN)

To configure Internet Group Management Protocol (IGMP) on a VLAN, use the **ip igmp snooping** command. To negate the command or return to the default settings, use the **no** form of this command

ip igmp snooping *parameter*

no ip igmp snooping *parameter*

Syntax Description

parameter	Parameter to configure. See the "Usage Guidelines" section for additional information.

Command Default

The default settings are as follows:

- **explicit-tracking**—enabled
- **fast-leave**—disabled for all VLANs
- **last-member-query-interval** *seconds*—1
- **querier** *IP-address*—disabled
- **report-suppression**—enabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Table 2-1 lists the valid values for *parameter*.

Table 2-1 IGMP Snooping Parameters

Keyword and Argument	Description
explicit-tracking	Enables tracking IGMPv3 membership reports for each port on a per-VLAN basis. The default is enabled on all VLANs.
fast-leave	Enables IGMPv3 snooping fast-leave processing. The default is disabled for all VLANs.
last-member-query-interval *seconds*	Removes the group if no hosts respond to an IGMP query message. Valid value is from 1 to 25 seconds. The default is 1 second.
mrouter interface *interface*	Configures a static connection to a multicast router. The specified interface is Ethernet or EtherChannel.
querier *IP-address*	Configures a snooping querier. The IP address is used as the source in messages. The default is disabled.

Send comments to nx5000-docfeedback@cisco.com

Table 2-1 IGMP Snooping Parameters (continued)

Keyword and Argument	Description
report-suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.
static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface*	Configures an interface belonging to a VLAN as a static member of a multicast group. The specified interface is Ethernet or EtherChannel.

Examples

This example shows how to configure IGMP snooping parameters for VLAN 5:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)# ip igmp snooping querier 192.168.2.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 192.168.1.1 interface ethernet 1/10
```

Related Commands

Command	Description
show ip igmp snooping	Displays the IGMP snooping information and configuration.

Send comments to nx5000-docfeedback@cisco.com

lacp port-priority

To set the priority for the physical interfaces for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command. To return the port priority to the default value, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Priority for the physical interfaces. The range of valid numbers is from 1 to 65535.

Command Default

System priority value is 32768.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Each port configured to use LACP has an LACP port priority. You can configure a value between 1 and 65535. LACP uses the port priority in combination with the port number to form the port identifier. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put into standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Note When setting the priority, note that a *higher* number means a *lower* priority.

Examples

This example shows how to set the LACP port priority for the interface to 2000:

```
switch(config-if)# lacp port-priority 2000
```

Related Commands

Command	Description
show lacp	Displays LACP information.

Send comments to nx5000-docfeedback@cisco.com

lacp rate fast

To configure the rate at which control packets are sent by the Link Aggregation Control Protocol (LACP), use the **lacp rate fast** command. To restore the rate to 30 seconds, use the **no** form of this command or the **lacp rate normal** command.

lacp rate fast

no lacp rate

no lacp rate fast

lacp rate normal

Syntax Description

This command has no arguments or keywords.

Command Default

1 second.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)N2(1)	This command was introduced.

Usage Guidelines

You must enable LACP before using this command.

You can configure the LACP rate fast feature on the LACP ports of a Cisco Nexus 5000 Series switch or a Cisco Nexus 2000 Series Fabric Extender that is connected to a Cisco Nexus 5000 Series switch.

The LACP rate fast feature is used to set the rate (once every second) at which the LACP control packets are sent to an LACP-supported interface. The normal rate at which LACP packets are sent is 30 seconds.

Examples

This example shows how to configure the LACP fast rate feature on a specified Ethernet interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# lacp rate fast
```

This example shows how to remove the LACP fast rate configuration from a specified Ethernet interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# no lacp rate fast
```

Related Commands

Command	Description
feature lacp	Enables or disables LACP on the switch.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
interface ethernet	Enters Ethernet interface configuration mode.
show lacp	Displays LACP configuration information.

Send comments to nx5000-docfeedback@cisco.com

lacp system-priority

To set the system priority of the switch for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command. To return the system priority to the default value, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	Priority for the physical interfaces. The range of valid numbers is from 1 to 65535.

Command Default

System priority value is 32768.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Each device that runs LACP has an LACP system priority value. You can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems.

When setting the priority, note that a *higher* number means a *lower* priority.

Examples

This example shows how to set the LACP system priority for the device to 2500:

```
switch(config)# lacp system-priority 2500
```

Related Commands

Command	Description
show lacp	Displays LACP information.

Send comments to nx5000-docfeedback@cisco.com

link debounce

To enable the debounce timer on an interface, use the **link debounce** command. To disable the timer, use the **no** form of this command.

link debounce [**time** *milliseconds*]

no link debounce

Syntax Description

time *milliseconds*	(Optional) Specifies the extended debounce timer. The range is from 0 to 5000 milliseconds. A value of 0 milliseconds disables the debounce time.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The port debounce time is the amount of time that an interface waits to notify the supervisor of a link going down. During this time, the interface waits to see if the link comes back up. The wait period is a time when traffic is stopped.

Caution When you enable the debounce timer, link up and link down detections are delayed, resulting in a loss of traffic during the debounce period. This situation might affect the convergence of some protocols.

Examples

This example shows how to enable the debounce timer and set the debounce time to 1000 milliseconds for an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# link debounce time 1000
```

This example shows how to disable the debounce timer for an Ethernet interface:

```
switch(config-if)# no link debounce
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show interface ethernet	Displays the interface configuration information.
show interface debounce	Displays the debounce time information for all interfaces.

Send comments to nx5000-docfeedback@cisco.com

mac address-table aging-time

To configure the aging time for entries in the MAC address table, use the **mac address-table aging-time** command. To return to the default settings, use the **no** form of this command.

mac address-table aging-time *seconds* [**vlan** *vlan-id*]

no mac address-table aging-time [**vlan** *vlan-id*]

Syntax Description

seconds	Aging time for MAC address table entries. The range is from 0 to 1000000 seconds. The default is 300 seconds. Entering 0 disables MAC address aging.
vlan *vlan-id*	(Optional) Specifies the VLAN to which the changed aging time should be applied.

Command Default

300 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **mac address-table aging-time**.

Usage Guidelines

Enter 0 seconds to disable the aging process.

The age value may be rounded off to the nearest multiple of 5 seconds. If the system rounds the value to a different value from that specified by the user (from the rounding process), the system returns an informational message.

When you use this command in EXEC mode, the age values of all VLANs for which a configuration has not been specified are modified and those VLANs with specifically modified aging times are not modified. When you use the **no** form of this command without the VLAN parameter, only those VLANs that have not been specifically configured for the aging time reset to the default value. Those VLANs with specifically modified aging times are not modified.

When you use this command and specify a VLAN, the aging time for only the specified VLAN is modified. When you use the **no** form of this command and specify a VLAN, the aging time for the VLAN is returned to the current global configuration for the aging time, which may or may not be the default value of 300 seconds depending if the global configuration of the switch for the aging time has been changed.

The aging time is counted from the last time that the switch detected the MAC address.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to change the length of time an entry remains in the MAC address table to 500 seconds for the entire switch:

```
switch(config)# mac address-table aging-time 500
```

Related Commands

Command	Description
show mac address-table	Displays information about the MAC address table.
show mac address-table aging-time	Displays information about the MAC address aging time.

Send comments to nx5000-docfeedback@cisco.com

mac address-table notification

To configure a log message notification of MAC address table events, use the **mac address-table notification** command. To disable log message notifications, use the **no** form of this command.

mac address-table notification {**mac-move** | **threshold** [**limit** *percentage* **interval** *seconds*]}

no mac address-table notification {**mac-move** | **threshold**}

Syntax Description

mac-move	Sends a notification message if the MAC address is moved.
threshold	Sends a notification message if the MAC address table threshold is exceeded.
limit *percentage*	(Optional) Specifies the percentage limit (1 to 100) beyond which threshold notifications are enabled.
interval *seconds*	(Optional) Specifies the minimum time in seconds (10 to 10000) between two notifications.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **mac address-table notification**.

Examples

This example shows how to configure a log message notification when the threshold exceeds 45 percent, restricting the update interval to once every 1024 seconds:

```
switch(config)# mac address-table notification threshold limit 45 interval 1024
```

Related Commands

Command	Description
show mac address-table	Displays information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

mac address-table static

To configure a static entry for the MAC address table, use the **mac address-table static** command. To delete the static entry, use the **no** form of this command.

mac address-table static *mac-address* **vlan** *vlan-id* {**drop** | **interface** {**ethernet** *slot*/*port* | **port-channel** *number*[**.***subinterface-number*]} [**auto-learn**]

no mac address-table static *mac-address* {**vlan** *vlan-id*}

Syntax Description

mac-address	MAC address to add to the table. Use the format EEEE.EEEE.EEEE.
vlan *vlan-id*	Specifies the VLAN to apply the static MAC address. The VLAN ID range is from 1 to 4094.
drop	Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
interface	Specifies the interface. The type can be either Ethernet or EtherChannel.
ethernet *slot*/*port*	Specifies the Ethernet interface and the appropriate slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
.subinterface-number	(Optional) EtherChannel number followed by a dot (.) indicator and the subinterface number.
auto-learn	(Optional) Allows the switch to automatically update this MAC address.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **mac address-table static**.

Usage Guidelines

You cannot apply the **mac address-table static** *mac-address* **vlan** *vlan-id* **drop** command to a multicast MAC address.

When you install a static MAC address, it is associated with a port. If the same MAC address is seen on a different port, the entry is updated with the new port if you enter the **auto-learn** keyword.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to add a static entry to the MAC address table:

```
switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 1/4
```

Related Commands

Command	Description
show mac address-table	Displays information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

monitor session

To create a new SPAN session configuration or add to an existing session configuration, use the **monitor session** command. To clear SPAN sessions, use the **no** form of this command.

monitor session {*session-number* [**shut** | **type local**] | **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.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **monitor session** {*session-number* | **all**} **suspend** command has been dropped. The **monitor session** {*session-number* | **all**} **shut** and **monitor session** {*session-number* | **all**} **type** commands have been added.

Usage Guidelines

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

Examples

This example shows how to create a SPAN session:

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

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 shut
```

Send comments to nx5000-docfeedback@cisco.com

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
```

Related Commands

Command	Description
show monitor session	Displays SPAN session configuration information.

Send comments to nx5000-docfeedback@cisco.com

name (VLAN configuration)

To set the name for a VLAN, use the **name** command. To remove the user-configured name from a VLAN, use the **no** form of this command.

name *vlan-name*

no name

Syntax Description

vlan-name	Name of the VLAN; you can use up to 32 alphanumeric, case-sensitive characters. The default name is VLAN*xxxx* where *xxxx* represents four numeric digits (including leading zeroes) equal to the VLAN ID number (for example, VLAN0002).

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You cannot change the name for the default VLAN, VLAN 1, or for the internally allocated VLANs.

Examples

This example shows how to name VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# name accounting
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

name (MST configuration)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

name	Name to assign to the MST region. It can be any string with a maximum length of 32 alphanumeric characters.

Command Default

None

Command Modes

MST configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Two or more switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Caution Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the switch in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# name accounting
```

Related Commands

Command	Description
show spanning-tree mst configuration	Displays information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration mode.

Send comments to nx5000-docfeedback@cisco.com

port-channel load-balance ethernet

To configure the load-balancing method among the interfaces in the channel-group bundle, use the **port-channel load-balance ethernet** command. To return the system priority to the default value, use the **no** form of this command.

port-channel load-balance ethernet *method*

no port-channel load-balance ethernet [*method*]

Syntax Description

method	Load-balancing method. See the "Usage Guidelines" section for a list of valid values.

Command Default

Loads distribution on the source and destination MAC address.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The valid load-balancing *method* values are as follows:

- **destination-ip**—Loads distribution on the destination IP address.
- **destination-mac**—Loads distribution on the destination MAC address.
- **destination-port**—Loads distribution on the destination port.
- **source-destination-ip**—Loads distribution on the source and destination IP address.
- **source-destination-mac**—Loads distribution on the source and destination MAC address.
- **source-destination-port**—Loads distribution on the source and destination port.
- **source-ip**—Loads distribution on the source IP address.
- **source-mac**—Loads distribution on the source MAC address.
- **source-port**—Loads distribution on the source port.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in that EtherChannel; using source addresses or IP addresses might result in better load balancing.

Examples

This example shows how to set the load-balancing method to use the source IP:

```
switch(config)# port-channel load-balance ethernet source-ip
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show port-channel load-balance	Displays information on EtherChannel load balancing.

Send comments to nx5000-docfeedback@cisco.com

private-vlan

To configure private VLANs, use the **private-vlan** command. To return the specified VLANs to normal VLAN mode, use the **no** form of this command.

private-vlan {**isolated** | **community** | **primary**}

no private-vlan {**isolated** | **community** | **primary**}

Syntax Description

isolated	Designates the VLAN as an isolated secondary VLAN.
community	Designates the VLAN as a community secondary VLAN.
primary	Designates the VLAN as the primary VLAN.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must enable private VLANs by using the **feature private-vlan** command before you can configure private VLANs. The commands for configuring private VLANs are not visible until you enable private VLANs.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. When you reconvert the specified VLAN to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. If you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and are reenabled when you recreate the specified VLAN and configure it as the previous secondary VLAN.

You cannot configure VLAN1 or the internally allocated VLANs as private VLANs.

A private VLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

An isolated VLAN is a VLAN that is used by isolated ports to communicate with promiscuous ports. An isolated VLAN's traffic is blocked on all other private ports in the same VLAN. Its traffic can only be received by standard trunking ports and promiscuous ports that are assigned to the corresponding primary VLAN.

A promiscuous port is defined as a private port that is assigned to a primary VLAN.

Send comments to nx5000-docfeedback@cisco.com

A community VLAN is defined as the VLAN that carries the traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

A primary VLAN is defined as the VLAN that is used to convey the traffic from the routers to customer end stations on private ports.

Multiple community and isolated VLANs are allowed. If you enter a range of primary VLANs, the system uses the first number in the range for the association.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

Examples

This example shows how to assign VLAN 5 to a private VLAN as the primary VLAN:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
```

This example shows how to assign VLAN 100 to a private VLAN as a community VLAN:

```
switch(config-vlan)# exit
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

This example shows how to assign VLAN 109 to a private VLAN as an isolated VLAN:

```
switch(config-vlan)# exit
switch(config)# vlan 109
switch(config-vlan)# private-vlan isolated
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
show vlan	Displays information about VLANs.
show vlan private-vlan	Displays information about private VLANs.

Send comments to nx5000-docfeedback@cisco.com

private-vlan association

To configure the association between a primary VLAN and a secondary VLAN on a private VLAN, use the **private-vlan association** command. To remove the association, use the **no** form of this command.

private-vlan association {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}

no private-vlan association

Syntax Description

add	(Optional) Associates a secondary VLAN to a primary VLAN.
secondary-vlan-list	Number of the secondary VLAN.
remove	Clears the association between a secondary VLAN and a primary VLAN.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must enable private VLANs by using the **feature private-vlan** command before you can configure private VLANs. The commands for configuring private VLANs are not visible until you enable private VLANs.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. However, when you reconvert the specified VLAN to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. However, if you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and return when you recreate the specified VLAN and configure it as the previous secondary VLAN.

The *secondary-vlan-list* argument cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single secondary VLAN ID or a hyphenated range of secondary VLAN IDs. The *secondary-vlan-list* parameter can contain multiple secondary VLAN IDs.

A private VLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

Multiple community and isolated VLANs are allowed. If you enter a range of primary VLANs, the system uses the first number in the range for the association.

Send comments to nx5000-docfeedback@cisco.com

Isolated and community VLANs can only be associated with one primary VLAN. You cannot configure a VLAN that is already associated to a primary VLAN as a primary VLAN.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

Examples

This example shows how to create a private VLAN relationship between the primary VLAN 14, the isolated VLAN 19, and the community VLANs 20 and 21:

```
switch(config)# vlan 19
switch(config-vlan)# private-vlan isolated
switch(config)# vlan 20
switch(config-vlan)# private-vlan community
switch(config)# vlan 21
switch(config-vlan)# private-vlan community
switch(config)# vlan 14
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 19-21
```

This example shows how to remove isolated VLAN 18 and community VLAN 20 from the private VLAN association:

```
switch(config)# vlan 14
switch(config-vlan)# private-vlan association remove 18,20
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
show vlan	Displays information about VLANs.
show vlan private-vlan	Displays information about private VLANs.

Send comments to nx5000-docfeedback@cisco.com

private-vlan synchronize

To map the secondary VLANs to the same Multiple Spanning Tree (MST) instance as the primary VLAN, use the **private-vlan synchronize** command.

private-vlan synchronize

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

MST configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you do not map secondary VLANs to the same MST instance as the associated primary VLAN when you exit the MST configuration mode, the device displays a warning message that lists the secondary VLANs that are not mapped to the same instance as the associated VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples

This example shows how to initialize private VLAN synchronization:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# private-vlan synchronize
```

Related Commands

Command	Description
show spanning-tree mst configuration	Displays information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration mode.

Send comments to nx5000-docfeedback@cisco.com

revision

To set the revision number for the Multiple Spanning Tree (MST) region configuration, use the **revision** command. To return to the default settings, use the **no** form of this command.

revision *version*

no revision *version*

Syntax Description

version	Revision number for the MST region configuration. The range is from 0 to 65535.

Command Default

Revision 0

Command Modes

MST configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Two or more switches with the same VLAN mapping and name are considered to be in different MST regions if the configuration revision numbers are different.

Caution Be careful when using the **revision** command to set the revision number of the MST region configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST region configuration:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
```

Related Commands

Command	Description
show spanning-tree mst	Displays information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

shutdown (VLAN configuration)

To shut down the local traffic on a VLAN, use the **shutdown** command. To return a VLAN to its default operational state, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Not shut down

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You cannot shut down, or disable, VLAN 1 or VLANs 1006 to 4094.

After you shut down a VLAN, the traffic ceases to flow on that VLAN. Access ports on that VLAN are also brought down; trunk ports continue to carry traffic for the other VLANs allowed on that port. However, the interface associations for the specified VLAN remain, and when you reenable, or recreate, that specified VLAN, the switch automatically reinstates all the original ports to that VLAN.

To find out if a VLAN has been shut down internally, check the Status field in the **show vlan** command output. If a VLAN is shut down internally, one of these values appears in the Status field:

- act/lshut—VLAN status is active and shut down internally.
- sus/lshut—VLAN status is suspended and shut down internally.

Note If the VLAN is suspended and shut down, you use both the **no shutdown** and **state active** commands to return the VLAN to the active state.

Examples

This example shows how to restore local traffic on VLAN 2 after you have shut down, or disabled, the VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# no shutdown
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree bpdufilter

To enable bridge protocol data unit (BPDU) Filtering on the interface, use the **spanning-tree bpdufilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter {**enable** | **disable**}

no spanning-tree bpdufilter

Syntax Description

enable	Enables BPDU Filtering on this interface.
disable	Disables BPDU Filtering on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree port type edge bpdufilter default** command.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Entering the **spanning-tree bpdufilter enable** command to enable BPDU Filtering overrides the spanning tree edge port configuration. That port then returns to the normal spanning tree port type and moves through the normal spanning tree transitions.

Caution Be careful when you enter the **spanning-tree bpdufilter enable** command on specified interfaces. Explicitly configuring BPDU Filtering on a port this is not connected to a host can cause a bridging loop because the port will ignore any BPDU that it receives, and the port moves to the STP forwarding state.

Use the **spanning-tree port type edge bpdufilter default** command to enable BPDU Filtering on all spanning tree edge ports.

Examples

This example shows how to explicitly enable BPDU Filtering on the Ethernet spanning tree edge port 1/4:

```
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdufilter enable
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) Guard on an interface, use the **spanning-tree bpduguard** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard {**enable** | **disable**}

no spanning-tree bpduguard

Syntax Description

enable	Enables BPDU Guard on this interface.
disable	Disables BPDU Guard on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree port type edge bpduguard default** command.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

BPDU Guard prevents a port from receiving BPDUs. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure.

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

When you enable this BPDU Guard command globally, the command applies only to spanning tree edge ports. See the **spanning-tree port type edge bpduguard default** command for more information on the global command for BPDU Guard. However, when you enable this feature on an interface, it applies to that interface regardless of the spanning tree port type.

This command has three states:

- **spanning-tree bpduguard enable**—Unconditionally enables BPDU Guard on the interface.
- **spanning-tree bpduguard disable**—Unconditionally disables BPDU Guard on the interface.
- **no spanning-tree bpduguard**—Enables BPDU Guard on the interface if it is an operational spanning tree edge port and if the **spanning-tree port type edge bpduguard default** command is configured.

Typically, this feature is used in a service-provider environment where the network administrator wants to prevent an access port from participating in the spanning tree.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to enable BPDU Guard on this interface:

```
switch(config-if)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command. To return to the default settings, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **cost** {*value* | **auto**}

no spanning-tree [**vlan** *vlan-id*] **cost**

Syntax Description

vlan *vlan-id*	(Optional) Lists the VLANs on this trunk interface for which you want to assign the path cost. You do not use this parameter on access ports. The range is from 1 to 4094.
value	Value of the port cost. The available cost range depends on the path-cost calculation method as follows: • short—The range is from 1 to 65536. • long—The range is from 1 to 200,000,000.
auto	Sets the value of the port cost by the media speed of the interface (see Table 2-2 for the values).

Command Default

Port cost is set by the media speed.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The STP port path cost default value is determined from the media speed and path cost calculation method of a LAN interface (see Table 2-2). See the **spanning-tree pathcost method** command for information on setting the path cost calculation method for Rapid per VLAN Spanning Tree Plus (Rapid PVST+).

Table 2-2 Default Port Cost

Bandwidth	Short Path Cost Method Port Cost	Long Path Cost Method Port Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1-Gigabit Ethernet	4	20,000
10-Gigabit Ethernet	2	2,000

When you configure the *value*, higher values will indicate higher costs.

Send comments to nx5000-docfeedback@cisco.com

On access ports, assign the port cost by port. On trunk ports, assign the port cost by VLAN; you can configure all the VLANs on a trunk port as the same port cost.

The EtherChannel bundle is considered as a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.

Note Use this command to set the port cost for Rapid PVST+. Use the **spanning-tree mst cost** command to set the port cost for MST.

Examples

This example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN that is associated with that interface:

```
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree cost 250
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree configuration.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree guard

To enable or disable Loop Guard or Root Guard, use the **spanning-tree guard** command. To return to the default settings, use the **no** form of this command.

spanning-tree guard {**loop** | **none** | **root**}

no spanning-tree guard

Syntax Description

loop	Enables Loop Guard on the interface.
none	Sets the guard mode to none.
root	Enables Root Guard on the interface.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You cannot enable Loop Guard if Root Guard is enabled, although the switch accepts the command to enable Loop Guard on **spanning tree edge ports**.

Examples

This example shows how to enable Root Guard:

```
switch(config-if)# spanning-tree guard root
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command. To return to the default settings, use the **no** form of this command.

spanning-tree link-type {**auto** | **point-to-point** | **shared**}

no spanning-tree link-type

Syntax Description

auto	Sets the link type based on the duplex setting of the interface.
point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Command Default

Link type set automatically based on the duplex setting.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Fast transition (specified in IEEE 802.1w) functions only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

Note On a Cisco Nexus 5000 Series switch, port duplex is not configurable.

Examples

This example shows how to configure the port as a shared link:

```
switch(config-if)# spanning-tree link-type shared
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree loopguard default

To enable Loop Guard as a default on all spanning tree normal and network ports, use the **spanning-tree loopguard default** command. To disable Loop Guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Loop Guard provides additional security in the bridge network. Loop Guard prevents alternate or root ports from becoming the designated port because of a failure that could lead to a unidirectional link.

Loop Guard operates only on ports that are considered point-to-point links by the spanning tree, and it does not run on spanning tree edge ports.

Entering the **spanning-tree guard loop** command for the specified interface overrides this global Loop Guard command.

Examples

This example shows how to enable Loop Guard:

```
switch(config)# spanning-tree loopguard default
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mode

To switch between Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) Spanning Tree Protocol (STP) modes, use the **spanning-tree mode** command. To return to the default settings, use the **no** form of this command.

spanning-tree mode {**rapid-pvst** | **mst**}

no spanning-tree mode

Syntax Description

rapid-pvst	Sets the STP mode to Rapid PVST+.
mst	Sets the STP mode to MST.

Command Default

Rapid PVST+

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You cannot simultaneously run MST and Rapid PVST+ on the switch.

Caution Be careful when using the **spanning-tree mode** command to switch between Rapid PVST+ and MST modes. When you enter the command, all STP instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause the user traffic to be disrupted.

Examples

This example shows how to switch to MST mode:

```
switch(config)# spanning-tree mode mst
switch(config-mst)#
```

Related Commands

Command	Description
show spanning-tree summary	Displays the information about the spanning tree configuration.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst configuration

To enter the Multiple Spanning Tree (MST) configuration mode, use the **spanning-tree mst configuration** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no keywords or arguments.

Command Default

The default value for the MST configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance. All VLANs are mapped to the Common and Internal Spanning Tree (CIST) instance.
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping—See the **instance vlan** command.
- Region name—See the **name (MST configuration)** command.
- Configuration revision number—See the **revision** command.

The **abort** and **exit** commands allow you to exit MST configuration mode. The difference between the two commands depends on whether you want to save your changes or not:

- The **exit** command commits all the changes before leaving MST configuration mode.
- The **abort** command leaves MST configuration mode without committing any changes.

If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST configuration mode, the following warning message is displayed:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

See the **switchport mode private-vlan host** command to fix this problem.

Changing an MST configuration mode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST configuration mode, make changes to a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the **exit** keyword.

Send comments to nx5000-docfeedback@cisco.com

In the unlikely event that two administrators commit a new configuration at exactly the same time, this warning message is displayed:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration mode:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)#
```

This example shows how to reset the MST configuration (name, instance mapping, and revision number) to the default settings:

```
switch(config)# no spanning-tree mst configuration
```

Related Commands

Command	Description
instance vlan	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst cost

To set the path-cost parameter for any Multiple Spanning Tree (MST) instance (including the Common and Internal Spanning Tree [CIST] with instance ID 0), use the **spanning-tree mst cost** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* **cost** {*cost* | **auto**}

no spanning-tree mst *instance-id* **cost**

Syntax Description

instance-id	Instance ID number. The range is from 0 to 4094.
cost	Port cost for an instance. The range is from 1 to 200,000,000.
auto	Sets the value of the port cost by the media speed of the interface.

Command Default

Automatically set port cost values:

- 10 Mbps—2,000,000
- 100 Mbps—200,000
- 1-Gigabit Ethernet—20,000
- 10-Gigabit Ethernet—2,000

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The port cost depends on the port speed; the faster interface speeds indicate smaller costs. MST always uses long path costs.

Higher cost values indicate higher costs. When entering the cost, do not include a comma in the entry; for example, enter 1000, not 1,000.

The EtherChannel bundle is considered as a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.

Examples

This example shows how to set the interface path cost:

```
switch(config-if)# spanning-tree mst 0 cost 17031970
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the switch, use the **spanning-tree mst forward-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Number of seconds to set the forward-delay timer for all the instances on the switch. The range is from 4 to 30 seconds.

Command Default

15 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to set the forward-delay timer:

```
switch(config)# spanning-tree mst forward-time 20
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the switch, use the **spanning-tree mst hello-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

seconds	Number of seconds to set the hello-time delay timer for all the instances on the switch. The range is from 1 to 10 seconds.

Command Default

2 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the hello-time delay timer:

```
switch(config)# spanning-tree mst hello-time 3
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst max-age

To set the max-age timer for all the instances on the switch, use the **spanning-tree mst max-age** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Number of seconds to set the max-age timer for all the instances on the switch. The range is from 6 to 40 seconds.

Command Default

20 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This parameter is used only by Instance 0 or the IST.

Examples

This example shows how to set the max-age timer:

```
switch(config)# spanning-tree mst max-age 40
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-tree mst max-hops** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Syntax Description

hop-count	Number of possible hops in the region before a BPDU is discarded. The range is from 1 to 255 hops.

Command Default

20 hops

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to set the number of possible hops:

```
switch(config)# spanning-tree mst max-hops 25
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst port-priority

To set the port-priority parameters for any Multiple Spanning Tree (MST) instance, including the Common and Internal Spanning Tree (CIST) with instance ID 0, use the **spanning-tree mst port-priority** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Syntax Description

instance-id	Instance ID number. The range is from 0 to 4094.
priority	Port priority for an instance. The range is from 0 to 224 in increments of 32.

Command Default

Port priority value is 128.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Higher **port-priority** *priority* values indicate smaller priorities.

The priority values are 0, 32, 64, 96, 128, 160, 192, and 224. All other values are rejected.

Examples

This example shows how to set the interface priority:

```
switch(config-if)# spanning-tree mst 0 port-priority 64
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Configures the port priority for the default STP, which is Rapid PVST+.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst priority

To set the bridge priority, use the **spanning-tree mst priority** command. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance-id* **priority** *priority-value*

no spanning-tree mst *instance-id* **priority**

Syntax Description

instance-id	Instance identification number. The range is from 0 to 4094.
priority-value	Bridge priority. See the “Usage Guidelines” section for valid values and additional information.

Command Default

Bridge priority default is 32768.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

You can set the *priority-value* argument to 0 to make the switch root.

You can enter the *instance-id* argument as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples

This example shows how to set the bridge priority:

```
switch(config)# spanning-tree mst 0 priority 4096
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst root

To designate the primary and secondary root and set the timer value for an instance, use the **spanning-tree mst root** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

instance-id	Instance identification number. The range is from 0 to 4094.
primary	Specifies the high priority (low value) that is high enough to make the bridge root of the spanning-tree instance.
secondary	Specifies the switch as a secondary root, if the primary root fails.
diameter *dia*	(Optional) Specifies the timer values for the bridge that are based on the network diameter.
hello-time *hello-time*	(Optional) Specifies the duration between the generation of configuration messages by the root switch. The range is from 1 to 10 seconds; the default is 2 seconds.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can enter the *instance-id* argument as a single instance or a range of instances, for example, 0-3,5,7-9.

If you do not specify the *hello-time* argument, the argument is calculated from the network diameter. You must first specify the **diameter** *dia* keyword and argument before you can specify the **hello-time** *hello-time* keyword and argument.

Examples

This example shows how to designate the primary root:

```
switch(config)# spanning-tree mst 0 root primary
```

This example shows how to set the priority and timer values for the bridge:

```
switch(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst simulate pvst

To reenable specific interfaces to automatically interoperate between Multiple Spanning Tree (MST) and Rapid per VLAN Spanning Tree Plus (Rapid PVST+), use the **spanning-tree mst simulate pvst** command. To prevent specific MST interfaces from automatically interoperating with a connecting device running Rapid PVST+, use the **spanning-tree mst simulate pvst disable** command. To return specific interfaces to the default settings that are set globally for the switch, use the **no** form of this command.

spanning-tree mst simulate pvst

spanning-tree mst simulate pvst disable

no spanning-tree mst simulate pvst

Syntax Description

This command has no keywords or arguments.

Command Default

Enabled. By default, all interfaces on the switch interoperate seamlessly between MST and Rapid PVST+. See the **spanning-tree mst simulate pvst global** command to change this setting globally.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

MST interoperates with Rapid PVST+ with no need for user configuration. The PVST+ simulation feature enables this seamless interoperability. However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a Rapid PVST+-enabled port.

When you use the **spanning-tree mst simulate pvst disable** command, specified MST interfaces that receive a Rapid PVST+ (SSTP) bridge protocol data unit (BPDU) move into the STP blocking state. Those interfaces remain in the inconsistent state until the port stops receiving Rapid PVST+ BPDUs, and then the port resumes the normal STP transition process.

Note To block automatic MST and Rapid PVST+ interoperability for the entire switch, use **no spanning-tree mst simulate pvst global** command.

This command is useful when you want to prevent accidental connection with a device running Rapid PVST+.

To reenable seamless operation between MST and Rapid PVST+ on specific interfaces, use the **spanning-tree mst simulate pvst** command.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to prevent specified ports from automatically interoperating with a connected device running Rapid PVST+:

```
switch(config-if)# spanning-tree mst simulate pvst disable
```

Related Commands

Command	Description
spanning-tree mst simulate pvst global	Enables global seamless interoperation between MST and Rapid PVST+.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst simulate pvst global

To prevent the Multiple Spanning Tree (MST) switch from automatically interoperating with a connecting device running Rapid per VLAN Spanning Tree Plus (Rapid PVST+), use the **spanning-tree mst simulate pvst global** command. To return to the default settings, which is a seamless operation between MST and Rapid PVST+ on the switch, use the **no spanning-tree mst simulate pvst global** command.

spanning-tree mst simulate pvst global

no spanning-tree mst simulate pvst global

Syntax Description

This command has no keywords or arguments.

Command Default

Enabled. By default, the switch interoperates seamlessly between MST and Rapid PVST+.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

MST does not require user configuration to interoperate with Rapid PVST+. The PVST+ simulation feature enables this seamless interoperability. However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a Rapid PVST+-enabled port.

When you use the **no spanning-tree mst simulate pvst global** command, the switch running in MST mode moves all interfaces that receive a Rapid PVST+ (SSTP) bridge protocol data unit (BPDU) into the Spanning Tree Protocol (STP) blocking state. Those interfaces remain in the inconsistent state until the port stops receiving Rapid PVST+ BPDUs, and then the port resumes the normal STP transition process.

You can also use this command from the interface mode, and the configuration applies to the entire switch.

Note To block automatic MST and Rapid PVST+ interoperability for specific interfaces, see the **spanning-tree mst simulate pvst** command.

This command is useful when you want to prevent accidental connection with a device not running MST.

To return the switch to seamless operation between MST and Rapid PVST+, use the **spanning-tree mst simulate pvst global** command.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to prevent all ports on the switch from automatically interoperating with a connected device running Rapid PVST+:

```
switch(config)# no spanning-tree mst simulate pvst global
```

Related Commands

Command	Description
spanning-tree mst simulate pvst	Enables seamless interoperation between MST and Rapid PVST+ by the interface.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

Syntax Description

long	Specifies the 32-bit based values for port path costs.
short	Specifies the 16-bit based values for port path costs.

Command Default

Short

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **long** path-cost calculation method uses all 32 bits for path-cost calculations and yields valued in the range of 2 through 2,00,000,000.

The **short** path-cost calculation method (16 bits) yields values in the range of 1 through 65535.

Note This command applies only to the Rapid per VLAN Spanning Tree Plus (Rapid PVST+) spanning tree mode, which is the default mode. When you are using Multiple Spanning Tree (MST) spanning tree mode, the switch uses only the long method for calculating path cost; this is not user-configurable for MST.

Examples

This example shows how to set the default pathcost method to long:

```
switch(config)# spanning-tree pathcost method long
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge

To configure an interface connected to a host as an edge port, which automatically transitions the port to the spanning tree forwarding state without passing through the blocking or learning states, use the **spanning-tree port type edge** command. To return the port to a normal spanning tree port, use the the **no spanning-tree port type** command.

spanning-tree port type edge [**trunk**]

no spanning-tree port type

Syntax Description

trunk	(Optional) Configures the trunk port as a spanning tree edge port.

Command Default

The default is the global setting for the default port type edge that is configured when you entered the **spanning-tree port type edge default** command. If you did not configure a global setting, the default spanning tree port type is normal.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can also use this command to configure a port in trunk mode as a spanning tree edge port.

Caution You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

When a linkup occurs, spanning tree edge ports are moved directly to the spanning tree forwarding state without waiting for the standard forward-time delay.

Note This is the same functionality that was previously provided by the Cisco-proprietary PortFast feature.

When you use this command, the system returns a message similar to the following:

```
Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
```

When you use this command without the **trunk** keyword, the system returns an additional message similar to the following:

```
%Portfast has been configured on Ethernet1/40 but will only
 have effect when the interface is in a non-trunking mode.
```

Send comments to nx5000-docfeedback@cisco.com

To configure trunk interfaces as spanning tree edge ports, use the **spanning-tree port type trunk** command. To remove the spanning tree edge port type setting, use the **no spanning-tree port type** command.

The default spanning tree port type is normal.

Examples

This example shows how to configure an interface connected to a host as an edge port, which automatically transitions that interface to the forwarding state on a linkup:

```
switch(config-if)# spanning-tree port type edge
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge bpdufilter default

To enable bridge protocol data unit (BPDU) Filtering by default on all spanning tree edge ports, use the **spanning-tree port type edge bpdufilter default** command. To disable BPDU Filtering by default on all edge ports, use the **no** form of this command.

spanning-tree port type edge bpdufilter default

no spanning-tree port type edge bpdufilter default

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To enable BPDU Filtering by default, you must do the following:

- Configure the interface as a spanning tree edge port, using the **spanning-tree port type edge** or the **spanning-tree port type edge default** command.
- Enable BPDU Filtering.

Use this command to enable BPDU Filtering globally on all spanning tree edge ports. BPDU Filtering prevents a port from sending or receiving any BPDUs.

Caution Be cautious when using this command; incorrect usage can cause bridging loops.

You can override the global effects of this **spanning-tree port type edge bpdufilter default** command by configuring BPDU Filtering at the interface level. See the **spanning-tree bpdufilter** command for complete information on using this feature at the interface level.

Note The BPDU Filtering feature's functionality is different when you enable it on a per-port basis or globally. When enabled globally, BPDU Filtering is applied only on ports that are operational spanning tree edge ports. Ports send a few BPDUs at a linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, that port immediately becomes a normal spanning tree port with all the normal transitions and BPDU Filtering is disabled. When enabled locally on a port, BPDU Filtering prevents the switch from receiving or sending BPDUs on this port.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to enable BPDU Filtering globally on all spanning tree edge operational ports by default:

```
switch(config)# spanning-tree port type edge bpdufilter default
```

Related Commands

Command	Description
show spanning-tree summary	Displays the information about the spanning tree configuration.
spanning-tree bpdufilter	Enables BPDU Filtering on the interface.
spanning-tree port type edge	Configures an interface as a spanning tree edge port.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge bpduguard default

To enable bridge protocol data unit (BPDU) Guard by default on all spanning tree edge ports, use the **spanning-tree port type edge bpduguard default** command. To disable BPDU Guard on all edge ports by default, use the **no** form of this command.

spanning-tree port type edge bpduguard default

no spanning-tree port type edge bpduguard default

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To enable BPDU Guard by default, you must do the following:

- Configure the interface as spanning tree edge ports by entering the **spanning-tree port type edge** or the **spanning-tree port type edge default** command.
- Enable BPDU Guard.

Use this command to enable BPDU Guard globally on all spanning tree edge ports. BPDU Guard disables a port if it receives a BPDU.

Global BPDU Guard is applied only on spanning tree edge ports.

You can also enable BPDU Guard per interface; see the **spanning-tree bpduguard** command for more information.

Note We recommend that you enable BPDU Guard on all spanning tree edge ports.

Examples

This example shows how to enable BPDU Guard by default on all spanning tree edge ports:

```
switch(config)# spanning-tree port type edge bpduguard default
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree summary	Displays the information about the spanning tree configuration.
spanning-tree bpduguard	Enables BPDU guard on the interface.
spanning-tree port type edge	Configures an interface as a spanning tree edge port.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge default

To configure all access ports that are connected to hosts as edge ports by default, use the **spanning-tree port type edge default** command. To restore all ports connected to hosts as normal spanning tree ports by default, use the **no** form of this command.

spanning-tree port type edge default

no spanning-tree port type edge default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to automatically configure all interfaces as spanning tree edge ports by default. This command will not work on trunk ports.

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

When a linkup occurs, an interface configured as an edge port automatically moves the interface directly to the spanning tree forwarding state without waiting for the standard forward-time delay. (This transition was previously configured as the Cisco-proprietary PortFast feature.)

When you use this command, the system returns a message similar to the following:

```
Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
```

You can configure individual interfaces as edge ports using the **spanning-tree port type edge** command.

The default spanning tree port type is normal.

Examples

This example shows how to globally configure all ports connected to hosts as spanning tree edge ports:

```
switch(config)# spanning-tree port type edge default
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree configuration.
spanning-tree port type edge	Configures an interface as a spanning tree edge port.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type network

To configure the interface that connects to a switch as a network spanning tree port, regardless of the global configuration, use the **spanning-tree port type network** command. To return the port to a normal spanning tree port, use the use the **no** form of this command.

spanning-tree port type network

no spanning-tree port type

Syntax Description

This command has no arguments or keywords.

Command Default

The default is the global setting for the default port type network that is configured when you entered the **spanning-tree port type network default** command. If you did not configure a global setting, the default spanning tree port type is normal.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to configure an interface that connects to a switch as a spanning tree network port. Bridge Assurance runs only on Spanning Tree Protocol (STP) network ports.

Note If you mistakenly configure ports connected to hosts as STP network ports and enable Bridge Assurance, those ports will automatically move into the blocking state.

Note Bridge Assurance is enabled by default, and all interfaces configured as spanning tree network ports have Bridge Assurance enabled.

To configure a port as a spanning tree network port, use the **spanning-tree port type network** command. To remove this configuration, use the **no spanning-tree port type** command. When you use the **no spanning-tree port type** command, the software returns the port to the global default setting for network port types.

You can configure all ports that are connected to switches as spanning tree network ports by default by entering the **spanning-tree port type network default** command.

The default spanning tree port type is normal.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to configure an interface connected to a switch or bridge as a spanning tree network port:

```
switch(config-if)# spanning-tree port type network
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning tree configuration per specified interface.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type network default

To configure all ports as spanning tree network ports by default, use the **spanning-tree port type network default** command. To restore all ports to normal spanning tree ports by default, use the **no** form of this command.

spanning-tree port type network default

no spanning-tree port type network default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to automatically configure all interfaces that are connected to switches as spanning tree network ports by default. You can then use the **spanning-tree port type edge** command to configure specified ports that are connected to hosts as spanning-tree edge ports.

Note If you mistakenly configure ports connected to hosts as Spanning Tree Protocol (STP) network ports and Bridge Assurance is enabled, those ports will automatically move into the blocking state.

Configure only the ports that connect to other switches as network ports because the Bridge Assurance feature causes network ports that are connected to hosts to move into the spanning tree blocking state.

You can identify individual interfaces as network ports by using the **spanning-tree port type network** command.

The default spanning tree port type is normal.

Examples

This example shows how to globally configure all ports connected to switches as spanning tree network ports:

```
switch(config)# spanning-tree port type network default
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree configuration.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port-priority

To set an interface priority when two bridges compete for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To return to the default settings, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **port-priority** *value*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

Syntax Description

vlan *vlan-id*	(Optional) Specifies the VLAN identification number. The range is from 0 to 4094.
value	Port priority. The range is from 1 to 224, in increments of 32.

Command Default

Port priority default value is 128.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Do not use the **vlan** *vlan-id* parameter on access ports. The software uses the port priority value for access ports and the VLAN port priority values for trunk ports.

The priority values are 0, 32, 64, 96, 128, 160, 192, and 224. All other values are rejected.

Note Use this command to configure the port priority for Rapid per VLAN Spanning Tree Plus (Rapid PVST+) spanning tree mode, which is the default STP mode. To configure the port priority for Multiple Spanning Tree (MST) spanning tree mode, use the **spacing-tree mst port-priority** command.

Examples

This example shows how to increase the probability that the spanning tree instance on access port interface 2/0 is chosen as the root bridge by changing the port priority to 32:

```
switch(config-if)# spanning-tree port-priority 32
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.
spanning-tree interface priority	Displays information on the spanning tree port priority for the interface.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree vlan

To configure Spanning Tree Protocol (STP) parameters on a per-VLAN basis, use the **spanning-tree vlan** command. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan-id* [**forward-time** *value* | **hello-time** *value* | **max-age** *value* | **priority** *value* | [**root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *value*]]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

Syntax Description

vlan-id	VLAN identification number. The VLAN ID range is from 0 to 4094.
forward-time *value*	(Optional) Specifies the STP forward-delay time. The range is from 4 to 30 seconds.
hello-time *value*	(Optional) Specifies the number of seconds between the generation of configuration messages by the root switch. The range is from 1 to 10 seconds.
max-age *value*	(Optional) Specifies the maximum number of seconds that the information in a bridge protocol data unit (BPDU) is valid. The range is from 6 to 40 seconds.
priority *value*	(Optional) Specifies the STP-bridge priority; the valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440. All other values are rejected.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Forces this switch to be the root switch if the primary root fails.
diameter *dia*	(Optional) Specifies the maximum number of bridges between any two points of attachment between end stations.

Command Default

The defaults are as follows:

- **forward-time**—15 seconds
- **hello-time**—2 seconds
- **max-age**—20 seconds
- **priority**—32768

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Send comments to nx5000-docfeedback@cisco.com

Usage Guidelines

Caution When disabling spanning tree on a VLAN using the **no spanning-tree vlan** *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.

Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When setting the **max-age** *seconds*, if a bridge does not see BPDUs from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

The **spanning-tree root primary** alters this switch's bridge priority to 24576. If you enter the **spanning-tree root primary** command and the switch does not become the root, then the bridge priority is changed to 4096 less than the bridge priority of the current bridge. The command fails if the value required to be the root bridge is less than 1. If the switch does not become the root, an error results.

If the network devices are set for the default bridge priority of 32768 and you enter the **spanning-tree root secondary** command, the software alters this switch's bridge priority to 28762. If the root switch fails, this switch becomes the next root switch.

Use the **spanning-tree root** commands on the backbone switches only.

Examples

This example shows how to enable spanning tree on VLAN 200:

```
switch(config)# spanning-tree vlan 200
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

speed (Ethernet)

To configure the transmit and receive speed for an Ethernet interface, use the **speed** command. To reset to the default speed, use the **no** form of this command.

speed {**1000** | **10000**}

no speed

Syntax Description

1000	Sets the interface speed to 1 Gbps.
10000	Sets the interface speed to 10 Gbps. This is the default speed.

Command Default

The default speed is 10000 (10-Gigabit).

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

The first 8 ports of a Nexus 5010 switch and the first 16 ports of a Nexus 5020 switch are switchable 1-Gigabit and 10-Gigabit ports. The default interface speed is 10-Gigabit. To configure these ports for 1-Gigabit Ethernet, insert a 1-Gigabit Ethernet SFP transceiver into the applicable port and then set its speed with the speed command.

Note If the interface and transceiver speed is mismatched, the SFP validation failed message is displayed when you enter the **show interface ethernet** *slot*/*port* command. For example, if you insert a 1-Gigabit SFP transceiver into a port without configuring the **speed 1000** command, you will get this error.

By default, all ports on a Cisco Nexus 5000 Series switch are 10 Gigabits.

Examples

This example shows how to set the speed for a 1-Gigabit Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# speed 1000
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send comments to nx5000-docfeedback@cisco.com

state

To set the operational state for a VLAN, use the **state** command. To return a VLAN to its default operational state, use the **no** form of this command.

state {**active** | **suspend**}

no state

Syntax Description

active	Specifies that the VLAN is actively passing traffic.
suspend	Specifies that the VLAN is not passing any packets.

Command Default

The VLAN is actively passing traffic.

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You cannot suspend the state for VLAN 1 or VLANs 1006 to 4094.

VLANs in the suspended state do not pass packets.

Examples

This example shows how to suspend VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# state suspend
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

svi enable

To enable the creation of VLAN interfaces, use the **svi enable** command. To disable the VLAN interface feature, use the **no** form of this command.

svi enable

no svi enable

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN interfaces are disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N1(1)	This command was deprecated and replaced with the **feature interface-vlan** command. For backwards compatibility, it will be maintained for a number of releases.

Usage Guidelines

You must use the **feature interface-vlan** command before you can create VLAN interfaces.

Examples

This example shows how to enable the interface VLAN feature on the switch:

```
switch(config)# svi enable
```

Related Commands

Command	Description
interface vlan	Creates a VLAN interface.

Send comments to nx5000-docfeedback@cisco.com

switchport access vlan

To set the access VLAN when the interface is in access mode, use the **switchport access vlan** command. To reset the access-mode VLAN to the appropriate default VLAN for the switch, use the **no** form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode. The range is from 1 to 4094, except for the VLANs reserved for internal use.

Command Default

VLAN 1

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **switchport access vlan** command to reset the access-mode VLAN to the appropriate default VLAN for the switch. This action may generate messages on the device to which the port is connected.

Examples

This example shows how to configure an Ethernet interface to join VLAN 2:

```
switch(config)# interface ethernet 1/7
switch(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a port.

Send comments to nx5000-docfeedback@cisco.com

switchport block

To prevent the unknown multicast or unicast packets from being forwarded, use the **switchport block** command. To allow the unknown multicast or unicast packets to be forwarded, use the **no** form of this command.

switchport block {**multicast** | **unicast**}

no switchport block {**multicast** | **unicast**}

Syntax Description

multicast	Specifies that the unknown multicast traffic should be blocked.
unicast	Specifies that the unknown unicast traffic should be blocked.

Command Default

Unknown multicast and unicast traffic are not blocked. All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can block the unknown multicast or unicast traffic on the switch ports.

Blocking the unknown multicast or unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.

Examples

This example shows how to block the unknown multicast traffic on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport block multicast
```

Related Commands

Command	Description
show interface switchport	Displays the switch port information for a specified interface or all interfaces.

Send comments to nx5000-docfeedback@cisco.com

switchport mode private-vlan host

To set the interface type to be a host port for a private VLAN, use the **switchport mode private-vlan host** command.

switchport mode private-vlan host

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When you configure a port as a host private VLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid private VLAN association configured.
- The port is a Switched Port Analyzer (SPAN) destination.
- The private VLAN association is suspended.

If you delete a private VLAN port association, or if you configure a private port as a SPAN destination, the deleted private VLAN port association or the private port that is configured as a SPAN destination becomes inactive.

Note We recommend that you enable spanning tree BPDU Guard on all private VLAN host ports.

Examples

This example shows how to set a port to host mode for private VLANs:

```
switch(config-if)# switchport mode private-vlan host
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
show vlan private-vlan	Displays the status of the private VLAN.

Send comments to nx5000-docfeedback@cisco.com

switchport mode private-vlan promiscuous

To set the interface type to be a promiscuous port for a private VLAN, use the **switchport mode private-vlan promiscuous** command.

switchport mode private-vlan promiscuous

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When you configure a port as a promiscuous private VLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid private VLAN mapping configured.
- The port is a Switched Port Analyzer (SPAN) destination.

If you delete a private VLAN port mapping or if you configure a private port as a SPAN destination, the deleted private VLAN port mapping or the private port that is configured as a SPAN destination becomes inactive.

See the **private-vlan** command for more information on promiscuous ports.

Examples

This example shows how to set a port to promiscuous mode for private VLANs:

```
switch(config-if)# switchport mode private-vlan promiscuous
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
show vlan private-vlan	Displays the status of the private VLAN.

Send comments to nx5000-docfeedback@cisco.com

switchport mode private-vlan trunk

To configure the port as a secondary trunk port for a private VLAN, use the **switchport mode private-vlan trunk** command. To remove the isolated trunk port, use the **no** form of this command.

switchport mode private-vlan trunk [**secondary**]

no switchport mode private-vlan trunk [**secondary**]

Syntax Description

secondary	(Optional) Specifies the secondary port.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

In a private VLAN domain, isolated trunks are part of a secondary VLAN. Isolated trunk ports can carry multiple isolated VLANs.

Examples

This example shows how to configure Ethernet interface 1/1 as a promiscuous trunk port for a private VLAN:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk secondary
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.

Send comments to nx5000-docfeedback@cisco.com

switchport private-vlan association trunk

To associate an isolated trunk port with the primary and secondary VLANs of a private VLAN, use the **switchport private-vlan association trunk** command. To remove the isolated trunk port association, use the **no** form of this command.

switchport private-vlan association trunk *primary-id secondary-id*

no switchport private-vlan association trunk

Syntax Description

primary-id	Primary VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.
secondary-id	Secondary VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The secondary VLAN should be an isolated VLAN. Only one isolated VLAN under a given primary VLAN can be associated to an isolated trunk port.

Examples

This example shows how to map the secondary VLANs to the primary VLAN:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk secondary
switch(config-if)# switchport private-vlan association trunk 5 100
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport mode private-vlan trunk	Configures the port as a secondary trunk port for a private VLAN.
show vlan private-vlan	Displays the status of the private VLAN.

Send comments to nx5000-docfeedback@cisco.com

switchport private-vlan trunk allowed vlan

To configure the allowed VLANs for the private trunk interface, use the **switchport private-vlan trunk allowed vlan** command. To remove the allowed VLANs, sue the **no** form of this command.

switchport private-vlan trunk allowed vlan {*vlan-list* | {**add** | **all** | **except** | **remove**} *vlan-list* | **none**}

no switchport private-vlan trunk allowed vlan {*vlan-list* | {**add** | **all** | **except** | **remove**} *vlan-list* | **none**}

Syntax Description

vlan-list	VLAN IDs of the allowed VLANs when the interface is in private-vlan trunking mode. The range is from 1 to 3967 and from 4048 to 4093. You can specify a list of VLAN IDs using the following separators: • **,** is a multirange separator; for example, 100-200, 201-203. • **-** is a range separator; for example, 100-200.
add	Specifies the VLANs to be added to the current list.
all	Specifies all VLANs to be added to the current list.
except	Specifies all VLANs to be added to the current list, except the specified VLANs.
remove	Specifies the VLANs to be removed from the current list.
none	Specifies that no VLANs be added to the current list.

Command Default

Allows only associated VLANs on the private VLAN trunk interface.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The primary VLANs do not need to be explicitly added to the allowed VLAN list. They are added automatically once there is a mapping between primary and secondary VLANs.

Examples

This example shows how to add VLANs to the list of allowed VLANs on an Ethernet private VLAN trunk port:

```
switch(config)# interface ethernet 1/3
switch(config-if)# switchport private-vlan trunk allowed vlan 15-20
switch(config-if)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport mode private-vlan trunk	Configures the port as a secondary trunk port for a private VLAN.
show vlan private-vlan	Displays the status of the private VLAN.

Send comments to nx5000-docfeedback@cisco.com

switchport private-vlan trunk native

To configure the native VLAN ID for the private VLAN trunk, use the **switchport private-vlan trunk native** command. To remove the native VLAN ID from the private VLAN trunk, use the **no** form of this command.

switchport private-vlan trunk native vlan *vlan-list*

no switchport private-vlan trunk native vlan *vlan-list*

Syntax Description

vlan *vlan-list*	Specifies the VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.

Command Default

VLAN 1.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Secondary VLANs cannot be configured with a native VLAN ID on promiscuous trunk ports. Primary VLANs cannot be configured with a native VLAN ID on isolated trunk ports.

Examples

This example shows how to map the secondary VLANs to the primary VLAN:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport private-vlan trunk native vlan 5
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport mode private-vlan trunk	Configures the port as a secondary trunk port for a private VLAN.
show vlan private-vlan	Displays the status of the private VLAN.

Send comments to nx5000-docfeedback@cisco.com

switchport host

To configure the interface to be an access host port, use the **switchport host** command. To remove the host port, use the **no** form of this command.

switchport host

no switchport host

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Ensure that you are configuring the correct interface. It must be an interface that is connnected to an end station.

An access host port handles the Spanning Tree Protocol (STP) like an edge port and immediately moves to the forwarding state without passing through the blocking and learning states. Configuring an interface as an access host port also disables EtherChannel on that interface.

Examples

This example shows how to set an interface as an Ethernet access host port with EtherChannel disabled:

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport host
switch(config-if)#
```

Related Commands

Command	Description
show interface brief	Displays a summary of the interface configuration information.
show interface switchport	Displays information on all interfaces configured as switch ports.

Send comments to nx5000-docfeedback@cisco.com

switchport mode

To configure the interface as a nontrunking nontagged single-VLAN Ethernet interface, use the **switchport mode** command. To remove the configuration and restore the default, use the **no** form of this command.

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

Syntax Description

access	Specifies that the interface is in access mode.
trunk	Specifies that the interface is in trunk mode.

Command Default

An access port carries traffic for VLAN 1.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

An access port can carry traffic in one VLAN only. By default,an access port carries traffic for VLAN 1. To set the access port to carry traffic for a different VLAN, use the **switchport access vlan** command.

The VLAN must exist before you can specify that VLAN as an access VLAN. The system shuts down an access port that is assigned to an access VLAN that does not exist.

Examples

This example shows how to set an interface as an Ethernet access port that carries traffic for a specific VLAN only:

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport access vlan	Sets the access VLAN when the interface is in access mode.

Send comments to nx5000-docfeedback@cisco.com

switchport private-vlan host-association

To define a private VLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the private VLAN association from the port, use the **no** form of this command.

switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan host-association

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-host mode. If the port is in private VLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive. The port also may be inactive when the association between the private VLANs is suspended.

The secondary VLAN may be an isolated or community VLAN.

See the **private-vlan** command for more information on primary VLANs, secondary VLANs, and isolated or community ports.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

Examples

This example shows how to configure a Layer 2 host private VLAN port with a primary VLAN (VLAN 18) and a secondary VLAN (VLAN 20):

```
switch(config-if)# switchport private-vlan host-association 18 20
```

This example shows how to remove the private VLAN association from the port:

```
switch(config-if)# no switchport private-vlan host-association
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show vlan private-vlan	Displays information on private VLANs.

Send comments to nx5000-docfeedback@cisco.com

switchport private-vlan mapping

To define the private VLAN association for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mapping from the primary VLAN, use the **no** form of this command.

switchport private-vlan mapping {*primary-vlan-id*} {[**add**] *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no switchport private-vlan mapping

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
add	(Optional) Associates the secondary VLANs to the primary VLAN.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.
remove	Clears the association between the secondary VLANs and the primary VLAN.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-promiscuous mode. If the port is in private VLAN-promiscuous mode but the primary VLAN does not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

See the **private-vlan** command for more information on primary VLANs, secondary VLANs, and isolated or community ports.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

Examples

This example shows how to configure the associated primary VLAN 18 to secondary isolated VLAN 20 on a private VLAN promiscuous port:

```
switch(config-if)# switchport private-vlan mapping 18 20
```

This example shows how to add a VLAN to the association on the promiscuous port:

```
switch(config-if)# switchport private-vlan mapping 18 add 21
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to remove all private VLAN associations from the port:

```
switch(config-if)# no switchport private-vlan mapping
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
show interface private-vlan mapping	Displays the information about the private VLAN mapping for VLAN interfaces or SVIs.

Send comments to nx5000-docfeedback@cisco.com

udld (configuration mode)

To configure the Unidirectional Link Detection (UDLD) protocol on the switch, use the **udld** command. To disable UDLD, use the **no** form of this command.

udld {**aggressive** | **message-time** *timer-time* | **reset**}

no udld {**aggressive** | **message-time** | **reset**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on the switch.
message-time *timer-time*	Sets the period of time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional. The range is from 7 to 90 seconds. The default is 15 seconds.
reset	Resets all the ports that are shut down by UDLD and permit traffic to begin passing through them again. Other features, such as spanning tree, will behave normally if enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

UDLD aggressive mode is disabled by default. You can configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. If UDLD aggressive mode is enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD frames, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

To prevent spanning tree loops, normal UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When you enable the UDLD aggressive mode, the following occurs:

- One side of a link has a port stuck (both transmission and receive)
- One side of a link remains up while the other side of the link is down

In these cases, the UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.

Examples

This example shows how to enable the aggressive UDLD mode for the switch:

```
switch# configure terminal
switch(config)# udld aggressive
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to reset all ports that were shut down by UDLD:

```
switch# configure terminal
switch(config)# udld reset
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.

Send comments to nx5000-docfeedback@cisco.com

udld (Ethernet)

To enable and configure the Unidirectional Link Detection (UDLD) protocol on an Ethernet interface, use the **udld** command. To disable UDLD, use the **no** form of this command.

udld {**aggressive** | **disable** | **enable**}

no udld {**aggressive** | **disable** | **enable**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on the interface.
disable	Disables UDLD on the interface.
enable	Enables UDLD in normal mode on the interface.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

You can configure normal or aggressive UDLD modes for an Ethernet interface. Before you can enable a UDLD mode for an interface, you must make sure that UDLD is enabled on the switch. UDLD must also be enabled on the other linked interface and its device.

To use the normal UDLD mode on a link, you must configure one of the ports for normal mode and configure the port on the other end for the normal or aggressive mode. To use the aggressive UDLD mode, you must configure both ends of the link for aggressive mode.

Examples

This example shows how to enable the normal UDLD mode for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# udld enable
```

This example shows how to enable the aggressive UDLD mode for an Ethernet port:

```
switch(config-if)# udld aggressive
```

This example shows how to disable UDLD for an Ethernet port:

```
switch(config-if)# udld disable
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.

Send comments to nx5000-docfeedback@cisco.com

vlan (EXEC mode)

To add a VLAN or to enter the VLAN configuration mode, use the **vlan** command. To delete the VLAN and exit the VLAN configuration mode, use the **no** form of this command.

vlan {*vlan-id* | *vlan-range*}

no vlan {*vlan-id* | *vlan-range*}

Syntax Description

vlan-id	Number of the VLAN. The range is from 1 to 4094. **Note** You cannot create, delete, or modify VLAN 1 or any of the internally allocated VLANs.
vlan-range	Range of configured VLANs; see the "Usage Guidelines" section for a list of valid values.

Command Default

None

Command Modes

Global configuration mode

Note You can also create and delete VLANs in the VLAN configuration mode using these same commands.

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When you enter the **vlan** *vlan-id* command, a new VLAN is created with all default parameters and causes the CLI to enter VLAN configuration mode. If the *vlan-id* argument that you entered matches an existing VLAN, nothing happens except that you enter VLAN configuration mode.

You can enter the *vlan-range* using a comma (**,**), a dash (**-**), and the number.

VLAN 1 parameters are factory configured and cannot be changed; you cannot create or delete this VLAN. Additionally, you cannot create or delete VLAN 4095 or any of the internally allocated VLANs.

When you delete a VLAN, all the access ports in that VLAN are shut down and no traffic flows. On trunk ports, the traffic continues to flow for the other VLANs allowed on that port, but the packets for the deleted VLAN are dropped. However, the system retains all the VLAN-to-port mapping for that VLAN, and when you reenable, or recreate, that specified VLAN, the switch automatically reinstates all the original ports to that VLAN.

Examples

This example shows how to add a new VLAN and enter VLAN configuration mode:

```
switch(config)# vlan 2
switch(config-vlan)#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to add a range of new VLANs and enter VLAN configuration mode:

```
switch(config)# vlan 2,5,10-12,20,25,4000
switch(config-vlan)#
```

This example shows how to delete a VLAN:

```
switch(config)# no vlan 2
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

vlan dot1Q tag native

To enable dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch, use the **vlan dot1Q tag native** command. To disable dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch, use the **no** form of this command.

vlan dot1Q tag native

no vlan dot1Q tag native

Syntax Description

This comand has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Typically, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN.

To maintain the tagging on the native VLAN and drop untagged traffic, use the **vlan dot1q tag native** command. The switch will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames, dropping any untagged traffic, including untagged traffic in the native VLAN.

Control traffic continues to be accepted as untagged on the native VLAN on a trunked port, even when the vlan dot1q tag native command is enabled.

Note The **vlan dot1q tag native** command is enabled on global basis

Examples

This example shows how to enable 802.1Q tagging on the switch:

```
switch(config)# vlan dot1q tag native
switch(config)#
```

This example shows how to disable 802.1Q tagging on the switch:

```
switch(config)# no vlan dot1q tag native
Turning off vlan dot1q tag native may impact the functioning of existing dot1q tunnel
ports
switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show vlan dot1q tag nativet	Displays the status of tagging on the native VLAN.

Send comments to nx5000-docfeedback@cisco.com

vrf context

To create a virtual routing and forwarding instance (VRF) and enter VRF configuration mode, use the **vrf context** command. To remove a VRF entry, use the **no** form of this command.

vrf context {*name* | **management**}

no vrf context {*name* | **management**}

Syntax Description

name	Name of the VRF. The name can be a maximum of 32 alphanumeric characters.
management	Specifies the management VRF.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When you enter the VRF configuration mode, the following commands are available:

- **exit**—Exits from the current command mode.
- **ip**—Enables configuration of IP features.

  Additional commands available in IP configuration mode:
  - **domain-list**—Adds additional domain names.
  - **domain-lookup**—Enables or disables DNS lookup.
  - **domain-name**—Specifies the default domain name.
  - **host**—Adds an entry to the IP hostname table
  - **name-server**—Specifies the IP address of a DNS name server
  - **route**—Adds route information by specifying IP addresses of the next hop servers.
- **no**—Negates a command or set its defaults.
- **shutdown**—Shuts down the current VRF context.

Examples

This example shows how to enter VRF context mode:

```
switch(config)# vrf context management
switch(config-vrf)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show vrf	Displays VRF information.

Send comments to nx5000-docfeedback@cisco.com

vtp domain

To configure the name of the VLAN Trunking Protocol (VTP) administrative domain, use the **vtp domain** command. To remove the domain name, use the **no** form of this command.

vtp domain *name*

no vtp domain

Syntax Description

name	VTP domain name. The name can be a maximum of 32 ASCII characters.

Command Default

Blank

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable VTP on the switch by using the **feature vtp** command.

Examples

This example shows how to create a VTP domain:

```
switch(config)# vtp domain accounting
switch(config)#
```

Related Commands

Command	Description
feature vtp	Enables VTP on the switch.
show vtp status	Displays VTP information.

Send comments to nx5000-docfeedback@cisco.com

vtp mode

To configure the VLAN Trunking Protocol (VTP) device mode, use the **vtp mode** command. To revert to the defaults, use the **no** form of this command.

vtp mode transparent

no vtp mode

Syntax Description

transparent	Specifies the device mode as transparent.

Command Default

Transparent

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to configure the VTP mode:

```
switch(config)# vtp mode transparent
switch(config)#
```

Related Commands

Command	Description
feature vtp	Enables VTP on the switch.
show vtp status	Displays VTP information.

Send comments to nx5000-docfeedback@cisco.com

vtp version

To configure the adminstrative domain to VLAN Trunking Protocol (VTP) version, use the **vtp version** command. To revert to the default version, use the **no** form of this command.

vtp version *version*

no vtp version

Syntax Description

version	VTP version. The range is from 1 to 2.

Command Default

Version 1 enabled

Version 2 disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable VTP on the switch by using the **feature vtp** command.

If you enable VTP, you must configure either version 1 or version 2. If you are using VTP in a Token Ring environment, you must use version 2.

Examples

This example shows how to create a VTP domain:

```
switch(config)# vtp version 2
switch(config)#
```

Related Commands

Command	Description
feature vtp	Enables VTP on the switch.
show vtp status	Displays VTP information.

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 3

Ethernet Show Commands

This chapter describes the Cisco NX-OS Ethernet **show** commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

show interface brief

To display a brief summary of the interface configuration information, use the **show interface brief** command.

show interface brief

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the summary configuration information of the specified interface:

```
switch# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth1/1        1      eth  trunk  up      none                       10G(D) 4000
Eth1/2        1      eth  trunk  up      none                       10G(D) 4000
Eth1/3        1      eth  trunk  up      none                       10G(D) 4000
Eth1/4        1      eth  trunk  up      none                       10G(D) 4000
Eth1/5        1      eth  access down    SFP not inserted           10G(D) --
Eth1/6        1      eth  access down    SFP not inserted           10G(D) --
Eth1/7        1      eth  trunk  up      none                       10G(D) 10
Eth1/8        1      eth  trunk  up      none                       10G(D) 10
Eth1/9        1      eth  trunk  up      none                       10G(D) 10
Eth1/10       1      eth  trunk  up      none                       10G(D) 10
Eth1/11       1      eth  access down    SFP not inserted           10G(D) --
Eth1/12       1      eth  access down    SFP not inserted           10G(D) --
Eth1/13       1      eth  access down    SFP not inserted           10G(D) --
Eth1/14       1      eth  access down    SFP not inserted           10G(D) --
Eth1/15       1      eth  access down    SFP not inserted           10G(D) --
Eth1/16       1      eth  access down    SFP not inserted           10G(D) --
Eth1/17       1      eth  access down    SFP not inserted           10G(D) --
Eth1/18       1      eth  access down    SFP not inserted           10G(D) --
Eth1/19       1      eth  access down    SFP not inserted           10G(D) --
Eth1/20       1      eth  access down    SFP not inserted           10G(D) --
Eth1/21       1      eth  access down    SFP not inserted           10G(D) --
Eth1/22       1      eth  access down    SFP not inserted           10G(D) --
Eth1/23       1      eth  access down    Link not connected         10G(D) --
Eth1/24       1      eth  access down    Link not connected         10G(D) --
Eth1/25       1      eth  access down    SFP not inserted           10G(D) --
Eth1/26       1      eth  access down    SFP not inserted           10G(D) --
Eth1/27       1      eth  access down    SFP not inserted           10G(D) --
```

Send comments to nx5000-docfeedback@cisco.com

```
Eth1/28       1      eth  access down    SFP not inserted           10G(D) --
Eth1/29       1      eth  access down    SFP not inserted           10G(D) --
Eth1/30       1      eth  access down    SFP not inserted           10G(D) --
Eth1/31       1      eth  access down    SFP not inserted           10G(D) --
Eth1/32       1      eth  access down    SFP not inserted           10G(D) --
Eth1/33       1      eth  access down    SFP not inserted           10G(D) --
Eth1/34       1      eth  access down    SFP not inserted           10G(D) --
Eth1/35       1      eth  access down    SFP not inserted           10G(D) --
Eth1/36       1      eth  access down    SFP not inserted           10G(D) --
Eth1/37       1      eth  access down    SFP not inserted           10G(D) --
Eth1/38       1      eth  access down    SFP not inserted           10G(D) --
Eth1/39       1      eth  access down    SFP not inserted           10G(D) --
Eth1/40       1      eth  trunk  up      none                       10G(D) --
Eth2/1        1      eth  access down    SFP not inserted           10G(D) --
Eth2/2        1      eth  access up      none                       10G(D) --
Eth2/3        1      eth  access down    SFP not inserted           10G(D) --
Eth2/4        1      eth  access up      none                       10G(D) --
Eth2/5        1      eth  access up      none                       10G(D) --
Eth2/6        1      eth  access down    SFP not inserted           10G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                   Speed  Protocol
Interface
--------------------------------------------------------------------------------
Po10         1     eth  trunk  up      none                      a-10G(D)  lacp
Po4000       1     eth  trunk  up      none                      a-10G(D)  lacp

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     192.168.10.37                           100      1500

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
--------------------------------------------------------------------------------
Vlan1     --                                      down   Administratively down

switch#
```

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.

Send comments to nx5000-docfeedback@cisco.com

show interface capabilities

To display detailed information about the capabilities of an interface, use the **show interface capabilities** command.

show interface ethernet *slot*/*port* **capabilities**

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can use the **show interface capabilities** command only for physical interfaces.

Examples

This example shows how to display the interface capabilities for a specific interface:

```
switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model:                N5K-C5020P-BF-XL-SU
  Type (SFP capable):   SFP-H10GB-CU1M
  Speed:                1000,10000
  Duplex:               full
  Trunk encap. type:    802.1Q
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:          rx-(off/on),tx-(off/on)
  Rate mode:            none
  QOS scheduling:       rx-(6q1t),tx-(1p6q0t)
  CoS rewrite:          no
  ToS rewrite:          no
  SPAN:                 yes
  UDLD:                 yes
  Link Debounce:        yes
  Link Debounce Time:   yes
  MDIX:                 no
  Pvlan Trunk capable:  yes
  TDR capable:          no
  Port mode:            Switched
  FEX Fabric:           yes

switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.

Send comments to nx5000-docfeedback@cisco.com

show interface debounce

To display the debounce time information for all interfaces, use the **show interface debounce** command.

show interface debounce

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the debounce status of all interfaces:

```
switch# show interface debounce

--------------------------------------------------------------------------------
Port          Debounce time   Value(ms)
--------------------------------------------------------------------------------
Eth1/1        enable              100
Eth1/2        enable              100
Eth1/3        enable              100
Eth1/4        enable              100
Eth1/5        enable              100
Eth1/6        enable              100
Eth1/7        enable              100
Eth1/8        enable              100
Eth1/9        enable              100
Eth1/10       enable              100
Eth1/11       enable              100
Eth1/12       enable              100
Eth1/13       enable              100
Eth1/14       enable              100
Eth1/15       enable              100
Eth1/16       enable              100
Eth1/17       enable              100
Eth1/18       enable              100
Eth1/19       enable              100
Eth1/20       enable              100
Eth1/21       enable              100
Eth1/22       enable              100
Eth1/23       enable              100
Eth1/24       enable              100
Eth1/25       enable              100
Eth1/26       enable              100
Eth1/27       enable              100
Eth1/28       enable              100
Eth1/29       enable              100
```

Send comments to nx5000-docfeedback@cisco.com

```
Eth1/30       enable              100
Eth1/31       enable              100
Eth1/32       enable              100
--More--
switch#
```

Related Commands

Command	Description
link debounce	Enables the debounce timer on an interface.

Send comments to nx5000-docfeedback@cisco.com

show interface ethernet

To display information about the interface configuration, use the **show interface ethernet** command.

show interface ethernet *slot/port* [**counters** | **description** | **status**]

Syntax Description

slot/port	Ethernet interface slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
counters	(Optional) Displays information about the counters configured on an interface.
description	(Optional) Displays the description of an interface configuration.
status	(Optional) Displays the operational state of the interface.

Command Default

Displays all information for the interface.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the detailed configuration of the specified interface:

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
  Hardware: 1000/10000 Ethernet, address: 000d.ece7.df48 (bia 000d.ece7.df48)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is fex-fabric
  full-duplex, 10 Gb/s, media type is 1/10g
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  Last link flapped 09:03:57
  Last clearing of "show interface" counters never
  30 seconds input rate 2376 bits/sec, 0 packets/sec
  30 seconds output rate 1584 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 1.58 Kbps, 0 pps; output rate 792 bps, 0 pps
  RX
    0 unicast packets  10440 multicast packets  0 broadcast packets
    10440 input packets  11108120 bytes
    0 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
```

Send comments to nx5000-docfeedback@cisco.com

```
  TX
    0 unicast packets  20241 multicast packets  105 broadcast packets
    20346 output packets  7633280 bytes
    0 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    0 Tx pause
  1 interface resets

switch#
```

This example shows how to display the counters configured on a specified interface:

```
switch# show interface ethernet 1/1 counters

--------------------------------------------------------------------------------
Port                InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Eth1/1              17193136                 0            16159                0
--------------------------------------------------------------------------------
Port               OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
Eth1/1           11576758                 0            28326              106
switch#
```

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.

Send comments to nx5000-docfeedback@cisco.com

show interface port-channel

To display the information about an EtherChannel interface configuration, use the **show interface port-channel** command.

show interface port-channel *number*[**.***subinterface-number*] [**brief** | **counters** | **description** | **status**]

Syntax Description

number	EtherChannel number. The range is from 1 to 4096.
.*subinterface-number*	(Optional) Port-channel subinterface configuration. Use the EtherChannel number followed by a dot (.) indicator and the subinterface number. The format is *portchannel-number***.***subinterface-number*.
counters	(Optional) Displays information about the counters configured on the EtherChannel interface.
description	(Optional) Displays the description of the EtherChannel interface configuration.
status	(Optional) Displays the operational state of the EtherChannel interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configuration information of a specified EtherChannel interface:

```
switch# show interface port-channel 21
port-channel21 is up
  Hardware: Port-Channel, address: 000d.ece7.df72 (bia 000d.ece7.df72)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s
  Beacon is turned off
  Input flow-control is on, output flow-control is on
  Switchport monitor is off
  Members in this channel: Eth2/3
  Last clearing of "show interface" counters never
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 352 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 368 bps, 0 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast packets
    0 input packets  0 bytes
```

Send comments to nx5000-docfeedback@cisco.com

```
    0 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    0 unicast packets  15813 multicast packets  9 broadcast packets
    15822 output packets  1615917 bytes
    0 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    0 Tx pause
  1 interface resets

switch#
```

Related Commands

Command	Description
interface port-channel	Configures an EtherChannel interface.

Send comments to nx5000-docfeedback@cisco.com

show interface mac-address

To display the information about the MAC address, use the **show interface mac-address** command.

show interface [*type slot*/*port* | *portchannel-no*] **mac-address**

Syntax Description

type	(Optional) Interface for which MAC addresses should be displayed. The *type* can be either Ethernet or EtherChannel.
slot/*port*	Ethernet interface port number and slot number. The slot number is from 1 to 255, and the port number is from 1 to 128.
portchannel-no	EtherChannel number. The EtherChannel number is from 1 to 4096.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you do not specify an interface, the system displays all the MAC addresses.

Examples

This example shows how to display the information on MAC addresses for the entire switch:

```
switch# show interface mac-address

--------------------------------------------------------------------------------
Interface                   Mac-Address     Burn-in Mac-Address
--------------------------------------------------------------------------------
Ethernet1/1                 0005.9b78.6e7c  0005.9b78.6e48
Ethernet1/2                 0005.9b78.6e7c  0005.9b78.6e49
Ethernet1/3                 0005.9b78.6e7c  0005.9b78.6e4a
Ethernet1/4                 0005.9b78.6e7c  0005.9b78.6e4b
Ethernet1/5                 0005.9b78.6e7c  0005.9b78.6e4c
Ethernet1/6                 0005.9b78.6e7c  0005.9b78.6e4d
Ethernet1/7                 0005.9b78.6e7c  0005.9b78.6e4e
Ethernet1/8                 0005.9b78.6e7c  0005.9b78.6e4f
Ethernet1/9                 0005.9b78.6e7c  0005.9b78.6e50
Ethernet1/10                0005.9b78.6e7c  0005.9b78.6e51
Ethernet1/11                0005.9b78.6e7c  0005.9b78.6e52
Ethernet1/12                0005.9b78.6e7c  0005.9b78.6e53
Ethernet1/13                0005.9b78.6e7c  0005.9b78.6e54
Ethernet1/14                0005.9b78.6e7c  0005.9b78.6e55
Ethernet1/15                0005.9b78.6e7c  0005.9b78.6e56
Ethernet1/16                0005.9b78.6e7c  0005.9b78.6e57
Ethernet1/17                0005.9b78.6e7c  0005.9b78.6e58
Ethernet1/18                0005.9b78.6e7c  0005.9b78.6e59
Ethernet1/19                0005.9b78.6e7c  0005.9b78.6e5a
```

Send comments to nx5000-docfeedback@cisco.com

```
Ethernet1/20              0005.9b78.6e7c  0005.9b78.6e5b
Ethernet1/21              0005.9b78.6e7c  0005.9b78.6e5c
Ethernet1/22              0005.9b78.6e7c  0005.9b78.6e5d
--More--
switch#
```

This example shows how to display the MAC address information for a specific port channel:

```
switch# show interface port-channel 5 mac-address

--------------------------------------------------------------------------------
Interface                 Mac-Address     Burn-in Mac-Address
--------------------------------------------------------------------------------
port-channel5             0005.9b78.6e7c  0005.9b78.6e7c
switch#
```

Related Commands

Command	Description
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
show mac address-table	Displays information on the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

show interface private-vlan mapping

To display information about private VLAN mapping for primary VLAN interfaces, use the **show interface private-vlan mapping** command.

show interface private-vlan mapping

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before you can configure private VLANs, you must enable them by using the **feature private-vlan** command. The commands for configuring private VLANs are not visible until you enable private VLANs.

This command displays the mapping information between the primary and secondary VLANs that allows both VLANs to share the VLAN interface of the primary VLAN.

Examples

This example shows how to display information about primary and secondary private VLAN mapping:

```
switch# show interface private-vlan mapping
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
show interface switchport	Displays information about the ports, including those in private VLANs.
show vlan	Displays summary information for all VLANs.
show vlan private-vlan	Displays information for all private VLANs on the device.

Send comments to nx5000-docfeedback@cisco.com

show interface status err-disabled

To display the error disabled state of interfaces, use the **show interface status err-disabled** command.

show interface status err-disabled

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the error disabled state of interfaces:

```
switch# show interface status err-disabled

--------------------------------------------------------------------------------
Port         Name               Status   Reason
--------------------------------------------------------------------------------
Eth114/1/27  --                 down     BPDUGuard errDisable
Eth114/1/28  --                 down     BPDUGuard errDisable
Eth114/1/29  --                 down     BPDUGuard errDisable
Eth114/1/30  --                 down     BPDUGuard errDisable
Eth114/1/31  --                 down     BPDUGuard errDisable
Eth114/1/32  --                 down     BPDUGuard errDisable
Eth114/1/33  --                 down     BPDUGuard errDisable
Eth114/1/34  --                 down     BPDUGuard errDisable
Eth114/1/35  --                 down     BPDUGuard errDisable
Eth114/1/36  --                 down     BPDUGuard errDisable
Eth114/1/39  --                 down     BPDUGuard errDisable
Eth114/1/40  --                 down     BPDUGuard errDisable
Eth114/1/41  --                 down     BPDUGuard errDisable
Eth114/1/42  --                 down     BPDUGuard errDisable
Eth114/1/43  --                 down     BPDUGuard errDisable
Eth114/1/44  --                 down     BPDUGuard errDisable
Eth114/1/45  --                 down     BPDUGuard errDisable
Eth114/1/46  --                 down     BPDUGuard errDisable
Eth114/1/47  --                 down     BPDUGuard errDisable
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
errdisable detect cause	Enables the errror disabled (err-disabled) detection.
errdisable recovery cause	Enables errror disabled recovery on an interface.

Send comments to nx5000-docfeedback@cisco.com

show interface switchport

To display information about all the switch port interfaces, use the **show interface switchport** command.

show interface switchport

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information for all Ethernet interfaces:

```
switch# show interface switchport
Name: Ethernet1/1
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: fex-fabric
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs:
  Operational private-vlan: none
  Unknown unicast blocked: disabled
  Unknown multicast blocked: disabled

Name: Ethernet1/2
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: fex-fabric
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
switchport access vlan	Sets the access VLAN when the interface is in access mode.

Send comments to nx5000-docfeedback@cisco.com

show interface transceiver

To display the information about the transceivers connected to a specific interface, use the **show interface transceiver** command.

show interface ethernet *slot*/*port* **transceiver** [**details**]

Syntax Description

ethernet *slot*/*port*	Displays information about an Ethernet interface slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
details	(Optional) Displays detailed information about the transceivers on an interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can use the **show interface transceiver** command only for physical interfaces.

Examples

This example shows how to display the transceivers connected to a specified Ethernet interface:

```
switch# show interface ethernet 1/1 transceiver
Ethernet1/1
    transceiver is present
    type is SFP-H10GB-CU1M
    name is CISCO-MOLEX
    part number is 74752-9044
    revision is 07
    serial number is MOC14081360
    nominal bitrate is 10300 MBit/sec
    Link length supported for copper is 1 m
    cisco id is --
    cisco extended id number is 4

switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.
show interface capabilities	Displays detailed information about the capabilities of an interface.

Send comments to nx5000-docfeedback@cisco.com

show interface vlan

To display brief descriptive information about specified VLANs, use the **show interface vlan** command.

show interface vlan *vlan-id* [**brief** | **private-vlan mapping**]

Syntax Description

vlan-id	Number of the VLAN. The range is from 1 to 4094.
brief	(Optional) Displays a summary information for the specified VLAN.
private-vlan mapping	(Optional) Displays the private VLAN mapping information, if any, for the specified VLAN.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must enable interface VLANs by using the **feature interface-vlan** or the **svi enable** command. The commands for configuring interface VLANs are not visible until you enable this feature.

This command displays descriptive information for the specified VLAN, including private VLANs.

The switch displays output for the **show interface vlan** *vlan-id* **private-vlan mapping** command only when you specify a primary private VLAN. If you specify a secondary private VLAN, the output is blank.

Examples

This example shows how to display information about the specified VLAN:

```
switch# show interface vlan 10
Vlan10 is up, line protocol is up
  Hardware is EtherSVI, address is  0005.9b78.6e7c
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,

switch#
```

This example shows how to display a brief description for the specified VLAN:

```
switch# show interface vlan 10 brief

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                   Status Reason
--------------------------------------------------------------------------------
Vlan10    --                                     up     --
switch#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the private VLAN mapping information, if any, for the VLAN:

```
switch# show interface vlan 10 private-vlan mapping
```

When you specify a primary VLAN, the switch displays all secondary VLANs mapped to that primary VLAN.

Related Commands

Command	Description
show interface switchport	Displays information about the ports, including those in private VLANs.
show vlan	Displays summary information for all VLANs.
show vlan private-vlan	Displays summary information for all private VLANs.

Send comments to nx5000-docfeedback@cisco.com

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the switch, use the **show ip igmp snooping** command.

show ip igmp snooping [**explicit-tracking vlan** *vlan-id* | **groups** [**detail** | **vlan** *vlan-id*] | **mrouter** [**vlan** *vlan-id*] | **querier** [**vlan** *vlan-id*] | **vlan** *vlan-id*]

Syntax Description

explicit-tracking	(Optional) Displays information about the explicit host-tracking status for IGMPv3 hosts. If you provide this keyword, you must specify a VLAN.
vlan *vlan-id*	(Optional) Specifies a VLAN. The VLAN ID range is from1 to 4094.
groups	(Optional) Displays information for the IGMP group address.
detail	(Optional) Displays detailed information for the group.
mrouter	(Optional) Displays information about dynamically detected multicast routers.
querier	(Optional) Displays information about the snooping querier if defined.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the IGMP snooping configuration of the switch:

```
switch# show ip igmp snooping
Global IGMP Snooping Information:
  IGMP Snooping enabled
  IGMPv1/v2 Report Suppression enabled
  IGMPv3 Report Suppression disabled
  Link Local Groups Suppression enabled

IGMP Snooping information for vlan 1
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 1
  Number of groups: 0
  VLAN vPC function enabled
  Active ports:
```

Send comments to nx5000-docfeedback@cisco.com

```
    Po19        Po400   Eth170/1/17     Eth171/1/7
    Eth171/1/8  Eth198/1/11     Eth199/1/13
IGMP Snooping information for vlan 300
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
--More--
switch#
```

Related Commands

Command	Description
ip igmp snooping (EXEC)	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping (VLAN)	Enables IGMP snooping on the VLAN interface.

Send comments to nx5000-docfeedback@cisco.com

show lacp

To display Link Aggregation Control Protocol (LACP) information, use the **show lacp** command.

show lacp {**counters** | **interface ethernet** *slot*/*port* | **neighbor** [**interface port-channel** *number*] | **port-channel** [**interface port-channel** *number*] | **system-identifier**}

Syntax Description

counters	Displays information about the LACP traffic statistics.
interface ethernet *slot*/*port*	Displays LACP information for a specific Ethernet interface. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
neighbor	Displays information about the LACP neighbor.
port-channel	Displays information about all EtherChannels.
interface port-channel *number*	(Optional) Displays information about a specific EtherChannel. The EtherChannel number is from 1 to 4096.
system-identifier	Displays the LACP system identification. It is a combination of the port priority and the MAC address of the device.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **show lacp** command to troubleshoot problems related to LACP in a network.

Examples

This example shows how to display the LACP system identification:

```
switch# show lacp system-identifier
32768,0-5-9b-78-6e-7c
switch#
```

This example shows how to display the LACP information for a specific interface:

```
switch# show lacp interface ethernet 1/1
Interface Ethernet1/1 is up
  Channel group is 1 port channel is Po1
  PDUs sent: 1684
  PDUs rcvd: 1651
  Markers sent: 0
  Markers rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
  Unknown packets rcvd: 0
  Illegal packets rcvd: 0
```

Send comments to nx5000-docfeedback@cisco.com

```
Lag Id: [ [(8000, 0-5-9b-78-6e-7c, 0, 8000, 101), (8000, 0-d-ec-c9-c8-3c, 0, 800
0, 101)] ]
Operational as aggregated link since Wed Apr 21 00:37:27 2010

Local Port: Eth1/1   MAC Address= 0-5-9b-78-6e-7c
  System Identifier=0x8000,0-5-9b-78-6e-7c
  Port Identifier=0x8000,0x101
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
  Partner information refresh timeout=Long Timeout (90s)
Actor Admin State=(Ac-1:To-1:Ag-1:Sy-0:Co-0:Di-0:De-0:Ex-0)
Actor Oper State=(Ac-1:To-0:Ag-1:Sy-1:Co-1:Di-1:De-0:Ex-0)
Neighbor: 1/1
  MAC Address= 0-d-ec-c9-c8-3c
  System Identifier=0x8000,0-d-ec-c9-c8-3c
  Port Identifier=0x8000,0x101
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
Partner Admin State=(Ac-0:To-1:Ag-0:Sy-0:Co-0:Di-0:De-0:Ex-0)
Partner Oper State=(Ac-1:To-0:Ag-1:Sy-1:Co-1:Di-1:De-0:Ex-0)
switch#
```

Related Commands

Command	Description
lacp port-priority	Sets the priority for the physical interfaces for the LACP.
lacp system-priority	Sets the system priority of the switch for the LACP.

Send comments to nx5000-docfeedback@cisco.com

show mac address-table aging-time

To display information about the time-out values for the MAC address table, use the **show mac address-table aging-time** command.

show mac address-table aging-time [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Displays information for a specific VLAN. The VLAN ID range is from 1 to 4094.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **show mac address-table aging-time**.

Examples

This example shows how to display MAC address aging times:

```
switch# show mac address-table aging-time
Vlan  Aging Time
----- ----------
2023  300
2022  300
2021  300
2020  300
2019  300
2018  300
2017  300
2016  300
2015  300
2014  300
2013  300
2012  300
2011  300
2010  300
2009  300
2008  300
2007  300
2006  300
2005  300
2004  300
2003  300
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
mac address-table aging-time	Configures the aging time for entries in the MAC address table.
show mac address-table	Displays information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

show mac address-table count

To display the number of entries currently in the MAC address table, use the **show mac address-table count** command.

show mac address-table count [**address** *EEEE.EEEE.EEEE*] [**dynamic** | **static**] [**interface** {**ethernet** *slot*/*port* | **port-channel** *number*}] [**vlan** *vlan-id*]

Syntax Description

address *EEEE.EEEE.EEEE*	(Optional) Displays a count of the MAC address table entries for a specific address.
dynamic	(Optional) Displays a count of the dynamic MAC addresses.
static	(Optional) Displays a count of the static MAC addresses.
interface	(Optional) Specifies the interface. The interface can be Ethernet or EtherChannel.
ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface. The EtherChannel number is from 1 to 4096.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **show mac address-table count**.

Examples

This example shows how to display the number of dynamic entries currently in the MAC address table:

```
switch# show mac address-table count dynamic
MAC Entries for all vlans:
Total MAC Addresses in Use: 7
switch#
```

Related Commands

Command	Description
show mac address-table	Displays information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

show mac address-table notification

To display notifications about the MAC address table, use the **show mac address-table notification** command.

show mac address-table notification {**mac-move** | **threshold**}

Syntax Description

mac-move	Displays notification messages about MAC addresses that were moved.
threshold	Displays notification messages sent when the MAC address table threshold was exceeded.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **show mac address-table notification**.

Examples

This example shows how to display MAC address move notifications:

```
switch# show mac address-table notification mac-move
MAC Move Notify : disabled
switch#
```

Related Commands

Command	Description
show mac address-table	Displays information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

show mac address-table

To display the information about the MAC address table, use the **show mac address-table** command.

show mac address-table [**address** *mac-address*] [**dynamic** | **multicast** | **static**] [**interface** {**ethernet** *slot*/*port* | **port-channel** *number*}] [**vlan** *vlan-id*]

Syntax Description

address *mac-address*	(Optional) Displays information about a specific MAC address.
dynamic	(Optional) Displays information about the dynamic MAC address table entries only.
interface	(Optional) Specifies the interface. The interface can be either Ethernet or EtherChannel.
ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface. The EtherChannel number is from 1 to 4096.
multicast	(Optional) Displays information about the multicast MAC address table entries only.
static	(Optional) Displays information about the static MAC address table entries only.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN. The VLAN ID range is from 1 to 4094.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The command syntax is changed to **show mac address-table**.

Usage Guidelines

The switch maintains static MAC address entries that are saved in its startup configuration across reboots and flushes the dynamic entries.

Examples

This example shows how to display information about the entries for the MAC address table:

```
switch# show mac address-table
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address      Type      age     Secure NTFY    Ports
---------+-----------------+--------+---------+------+----+------------------
```

Send comments to nx5000-docfeedback@cisco.com

```
+ 100      0000.0001.0003    dynamic   0          F    F  Po1
+ 100      0000.0001.0004    dynamic   0          F    F  Po1
+ 100      0000.0001.0009    dynamic   0          F    F  Po1
+ 100      0000.0001.0010    dynamic   0          F    F  Po1
* 1        001d.7172.6c40    dynamic   300        F    F  Eth100/1/20
switch#
```

This example shows how to display information about the entries for the MAC address table for a specific MAC address:

```
switch# show mac address-table address 0018.bad8.3fbd
```

This example shows how to display information about the dynamic entries for the MAC address table:

```
switch# show mac address-table dynamic
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address      Type      age     Secure NTFY    Ports
---------+-----------------+--------+---------+------+----+------------------
+ 100      0000.0001.0003    dynamic   0          F    F  Po1
+ 100      0000.0001.0004    dynamic   0          F    F  Po1
+ 100      0000.0001.0009    dynamic   0          F    F  Po1
+ 100      0000.0001.0010    dynamic   0          F    F  Po1
* 1        001d.7172.6c40    dynamic   300        F    F  Eth100/1/20
switch#
```

This example shows how to display information about the MAC address table for a specific interface:

```
switch# show mac address-table interface ethernet 1/3
```

This example shows how to display static entries in the MAC address table:

```
switch# show mac address-table static
```

This example shows how to display entries in the MAC address table for a specific VLAN:

```
switch# show mac address-table vlan 1
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address      Type      age     Secure NTFY    Ports
---------+-----------------+--------+---------+------+----+------------------
* 1        001d.7172.6c40    dynamic   60         F    F  Eth100/1/20
switch#
```

Related Commands

Command	Description
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
show mac address-table aging-time	Displays information about the time-out values for the MAC address table.
show mac address-table count	Displays the number of entries currently in the MAC address table.
show mac address-table notifications	Displays information about notifications for the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

show monitor session

To display information about the Switched Port Analyzer (SPAN) 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.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information about SPAN session 1:

```
switch# show monitor session 1
```

This example shows how to display a range of SPAN sessions:

```
switch# show monitor session range 1-4
```

Related Commands

Command	Description
monitor session	Displays the contents of the startup configuration file.

Send comments to nx5000-docfeedback@cisco.com

show port-channel capacity

To display the total number of EtherChannel interfaces and the number of free or used EtherChannel interfaces, use the **show port-channel capacity** command.

show port-channel capacity

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the EtherChannel capacity:

```
switch# show port-channel capacity
Port-channel resources
    768 total    29 used    739 free    3% used
switch#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for EtherChannels.
show tech-support port-channel	Displays Cisco Technical Support information about EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

show port-channel compatibility-parameters

To display the parameters that must be the same among the member ports in order to join an EtherChannel interface, use the **show port-channel compatibility-parameters** command.

show port-channel compatibility-parameters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the EtherChannel interface parameters:

```
switch# show port-channel compatibility-parameters
* port mode

Members must have the same port mode configured.

* port mode

Members must have the same port mode configured, either E,F or AUTO. If
they are configured in AUTO port mode, they have to negotiate E or F mode
when they come up. If a member negotiates a different mode, it will be
suspended.

* speed

Members must have the same speed configured. If they are configured in AUTO
speed, they have to negotiate the same speed when they come up. If a member
negotiates a different speed, it will be suspended.

* MTU

Members have to have the same MTU configured. This only applies to ethernet
port-channel.

* shut lan

Members have to have the same shut lan configured. This only applies to
ethernet port-channel.

* MEDIUM

Members have to have the same medium type configured. This only applies to
ethernet port-channel.
```

Send comments to nx5000-docfeedback@cisco.com

```
* Span mode

Members must have the same span mode.

* load interval

Member must have same load interval configured.
--More--
<---output truncated--->
switch#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for EtherChannels.
show tech-support port-channel	Displays Cisco Technical Support information about EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

show port-channel database

To display the aggregation state for one or more EtherChannel interfaces, use the **show port-channel database** command.

show port-channel database [**interface port-channel** *number*[**.***subinterface-number*]]

Syntax Description

interface	(Optional) Displays information for an EtherChannel interface.
port-channel *number*	(Optional) Displays aggregation information for a specific EtherChannel interface. The *number* range is from 1 to 4096.
.*subinterface-number*	(Optional) Subinterface number. Use the EtherChannel number followed by a dot (.) indicator and the subinterface number. The format is *portchannel-number***.***subinterface-number*.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the aggregation state of all EtherChannel interfaces:

```
switch# show port-channel database
port-channel19
    Last membership update is successful
    4 ports in total, 4 ports up
    First operational port is Ethernet199/1/24
    Age of the port-channel is 0d:09h:11m:30s
    Time since last bundle is 0d:09h:12m:20s
    Last bundled member is
    Ports:   Ethernet199/1/24  [active ] [up] *
             Ethernet199/1/28  [active ] [up]
             Ethernet199/1/30  [active ] [up]
             Ethernet199/1/31  [active ] [up]

port-channel21
    Last membership update is successful
    1 ports in total, 1 ports up
    First operational port is Ethernet2/3
    Age of the port-channel is 0d:09h:11m:30s
    Time since last bundle is 0d:09h:12m:20s
    Last bundled member is
    Ports:   Ethernet2/3     [on] [up] *

port-channel50
    Last membership update is successful
--More--
<---output truncated--->
```

Send comments to nx5000-docfeedback@cisco.com

```
switch#
```

This example shows how to display the aggregation state for a specific EtherChannel interface:

```
switch# show port-channel database interface port-channel 21
port-channel21
    Last membership update is successful
    1 ports in total, 1 ports up
    First operational port is Ethernet2/3
    Age of the port-channel is 0d:09h:13m:14s
    Time since last bundle is 0d:09h:14m:04s
    Last bundled member is
    Ports:   Ethernet2/3     [on] [up] *

switch#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for EtherChannels.
show tech-support port-channel	Displays Cisco Technical Support information about EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

show port-channel load-balance

To display information about EtherChannel load balancing, use the **show port-channel load-balance** command.

show port-channel load-balance [**forwarding-path interface port-channel** *number* {**.** | **vlan** *vlan_ID*} [**dst-ip** *ipv4-addr*] [**dst-ipv6** *ipv6-addr*] [**dst-mac** *dst-mac-addr*] [**l4-dst-port** *dst-port*] [**l4-src-port** *src-port*] [**src-ip** *ipv4-addr*] [**src-ipv6** *ipv6-addr*] [**src-mac** *src-mac-addr*]]

Syntax Description

forwarding-path interface port-channel	(Optional) Identifies the port in the EtherChannel interface that forwards the packet.
number	EtherChannel number for the load-balancing forwarding path that you want to display. The range is from 1 to 4096.
.	(Optional) Subinterface number separator. Use the EtherChannel number followed by a dot (.) indicator and the subinterface number. The format is *portchannel-number.subinterface-number*.
vlan	(Optional) Identifies the VLAN for hardware hashing.
vlan_ID	VLAN ID. The range is from 1 to 3967 and 4048 to 4093.
dst-ip	(Optional) Displays the load distribution on the destination IP address.
ipv4-addr	IPv4 address to specify a source or destination IP address. The format is *A.B.C.D*.
dst-ipv6	(Optional) Displays the load distribution on the destination IPv6 address.
ipv6-addr	IPv6 address to specify a source or destination IP address. The format is *A*:*B*::*C*:*D*.
dst-mac	(Optional) Displays the load distribution on the destination MAC address.
dst-mac-addr	Destination MAC address. The format is *AAAA*:*BBBB*:*CCCC*.
l4-dst-port	(Optional) Displays the load distribution on the destination port.
dst-port	Destination port number. The range is from 0 to 65535.
l4-src-port	(Optional) Displays the load distribution on the source port.
src-port	Source port number. The range is from 0 to 65535.
src-ip	(Optional) Displays the load distribution on the source IP address.
src-ipv6	(Optional) Displays the load distribution on the source IPv6 address.
src-mac	(Optional) Displays the load distribution on the source MAC address.
src-mac-addr	source MAC address. The format is *AA*:*BB*:*CC*:*DD*:*EE*:*FF*.

Command Default

None

Command Modes

EXEC mode

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **vlan** keyword was added.

Usage Guidelines

You must use the **vlan** keyword to determine the use of hardware hashing.

When you do not use hardware hashing, the output displays all parameters used to determine the outgoing port ID. Missing parameters are shown as zero values in the output.

If you do not use hardware hashing, the outgoing port ID is determined by using control-plane selection. Hardware hashing is not used in the following scenarios:

- The specified VLAN contains an unknown unicast destination MAC address.
- The specified VLAN contains a known or an unknown multicast destination MAC or destination IP address.
- The specified VLAN contains a broadcast MAC address.
- The EtherChannel has only one active member.
- The destination MAC address is unknown when the load distribution is configured on the source IP address (src-ip), source port (l4-src-port), or source MAC address (src-mac).
- If multichassis EtherChannel trunk (MCT) is enabled and the traffic flows from a virtual port channel (vPC) peer link, the output displays “Outgoing port id (vPC peer-link traffic)”.

To get accurate results, you must do do the following:

- (For unicast frames) Provide the destination MAC address (dst-mac) and the VLAN for hardware hashing (vlan). When the destination MAC address is not provided, hardware hashing is assumed.
- (For multicast frames) For IP multicast, provide either the destination IP address (dst-ip) or destination MAC address (dst-mac) with the VLAN for hardware hashing (vlan). For non-ip multicast, provide the destination MAC address with the VLAN for hardware hashing.
- (For broadcast frames) Provide the destination MAC address (dst-mac) and the VLAN for hardware hashing (vlan).

Examples

This example shows how to display the port channel load balance information:

```
switch# show port-channel load-balance
Port Channel Load-Balancing Configuration:
System: source-dest-ip

Port Channel Load-Balancing Addresses Used Per-Protocol:
Non-IP: source-dest-mac
IP: source-dest-ip source-dest-mac

switch#
```

Table 3-1 describes the fields shown in the display:

Send comments to nx5000-docfeedback@cisco.com

Table 3-1 show port-channel load-balance Field Descriptions

Field	Description
System	The load-balancing method configured on the switch.
Non-IP	The field that will be used to calculate the hash value for non-IP traffic.
IP	The fileds used for IPv4 and IPv6 traffic.

This example shows how to display the port channel load balance information when hardware hashing is not used:

```
switch# show port-channel load-balance forwarding-path interface port-channel 5 vlan 3
dst-ip 192.168.2.37
Missing params will be substituted by 0's.
Load-balance Algorithm on FEX: source-dest-ip
crc8_hash: Not Used     Outgoing port id: Ethernet133/1/3
Param(s) used to calculate load-balance (Unknown unicast, multicast and broadcas
t packets):
        dst-mac:  0000.0000.0000
        vlan id:  3
switch#
```

This example shows how to display the port channel load balance information when hardware hashing is not used to determine the outgoing port ID:

```
switch# show port-channel load-balance forwarding-path interface port-channel 10 vlan 1
dst-ip 192.168.2.25 src-ip 192.168.2.10 dst-mac ffff.ffff.ffff src-mac aa:bb:cc:dd:ee:ff
l4-src-port 0 l4-dst-port 1
Missing params will be substituted by 0's.
Load-balance Algorithm on switch: source-dest-port
crc8_hash: Not Used     Outgoing port id: Ethernet1/1
Param(s) used to calculate load-balance (Unknown unicast, multicast and broadcast
packets):
        dst-mac:  ffff.ffff.ffff
        vlan id:  1

switch#
```

This example shows how to display the port channel load balance information when MCT is enabled and traffic flows from a vPC peer link:

```
switch# show port-channel load-balance forwarding-path interface port-channel 10 vlan 1
dst-ip 192.168.2.25 src-ip 192.168.2.10 dst-mac ffff.ffff.ffff src-mac aa:bb:cc:dd:ee:ff
l4-src-port 0 l4-dst-port 1
Missing params will be substituted by 0's.
Load-balance Algorithm on switch: source-dest-port
crc8_hash: Not Used     Outgoing port id (non vPC peer-link traffic): ethernet1/2
crc8_hash: Not Used     Outgoing port id (vPC peer-link traffic): Ethernet1/1
Param(s) used to calculate load-balance (Unknown unicast, multicast and broadcast
packets):
        dst-mac:  ffff.ffff.ffff
        vlan id:  1

switch#
```

This example shows how to display the port channel load balance information when hardware hashing is used to determine the outgoing port ID:

Send comments to nx5000-docfeedback@cisco.com

```
switch# show port-channel load-balance forwarding-path interface port-channel 10 vlan 1
dst-ip 192.168.2.25 src-ip 192.168.2.10 src-mac aa:bb:cc:dd:ee:ff l4-src-port 0
l4-dst-port 1
Missing params will be substituted by 0's.
Load-balance Algorithm on switch: source-dest-port
crc8_hash: 204  Outgoing port id: Ethernet1/1
Param(s) used to calculate load-balance:
        dst-port: 1
        src-port: 0
        dst-ip:   192.168.2.25
        src-ip:   192.168.2.10
        dst-mac:  0000.0000.0000
       src-mac:  aabb.ccdd.eeff

switch#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing method among the interfaces in the channel-group bundle.

Send comments to nx5000-docfeedback@cisco.com

show port-channel summary

To display summary information about EtherChannels, use the **show port-channel summary** command.

show port-channel summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before you use this command, you must configure an EtherChannel group using the **interface port-channel** command.

Examples

This example shows how to display summary information about EtherChannels:

```
switch# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth1/1(P)    Eth1/2(P)    Eth1/3(P)
                                     Eth1/4(P)    Eth1/21(P)   Eth1/22(P)
                                     Eth1/23(P)   Eth1/24(P)   Eth1/25(P)
                                     Eth1/26(P)   Eth1/27(P)   Eth1/28(P)
                                     Eth1/29(P)   Eth1/30(P)   Eth1/31(P)
                                     Eth1/32(P)
3     Po3(SU)     Eth      NONE      Eth1/9(P)    Eth1/10(P)   Eth1/13(P)
                                     Eth1/14(P)   Eth1/40(P)
5     Po5(SU)     Eth      NONE      Eth3/5(P)    Eth3/6(P)
6     Po6(SU)     Eth      NONE      Eth1/5(P)    Eth1/6(P)    Eth1/7(P)
                                     Eth1/8(P)
12    Po12(SU)    Eth      NONE      Eth3/3(P)    Eth3/4(P)
15    Po15(SD)    Eth      NONE      --
20    Po20(SU)    Eth      NONE      Eth1/17(P)   Eth1/18(P)   Eth1/19(D)
                                     Eth1/20(P)
24    Po24(SU)    Eth      LACP      Eth105/1/27(P)  Eth105/1/28(P)  Eth105/1/29
(P)
```

Send comments to nx5000-docfeedback@cisco.com

```
                                        Eth105/1/30(P)  Eth105/1/31(P)  Eth105/1/32
(P)
25    Po25(SU)    Eth      LACP      Eth105/1/23(P)  Eth105/1/24(P)  Eth105/1/25
(P)
                                        Eth105/1/26(P)
33    Po33(SD)    Eth      NONE      --
41    Po41(SD)    Eth      NONE      --
44    Po44(SD)    Eth      NONE      --
48    Po48(SD)    Eth      NONE      --
100   Po100(SD)   Eth      NONE      --
101   Po101(SD)   Eth      NONE      --
102   Po102(SU)   Eth      LACP      Eth102/1/2(P)
103   Po103(SU)   Eth      LACP      Eth102/1/3(P)
104   Po104(SU)   Eth      LACP      Eth102/1/4(P)
105   Po105(SU)   Eth      LACP      Eth102/1/5(P)
106   Po106(SU)   Eth      LACP      Eth102/1/6(P)
107   Po107(SU)   Eth      LACP      Eth102/1/7(P)
108   Po108(SU)   Eth      LACP      Eth102/1/8(P)
109   Po109(SU)   Eth      LACP      Eth102/1/9(P)
110   Po110(SU)   Eth      LACP      Eth102/1/10(P)
111   Po111(SU)   Eth      LACP      Eth102/1/11(P)
<---output truncated--->
switch#
```

Related Commands

Command	Description
channel-group (Ethernet)	Assigns and configures a physical interface to an EtherChannel.
interface port-channel	Creates an EtherChannel interface and enters interface configuration mode.

Send comments to nx5000-docfeedback@cisco.com

show port-channel traffic

To display the traffic statistics for EtherChannels, use the **show port-channel traffic** command.

show port-channel traffic [**interface port-channel** *number*[**.***subinterface-number*]]

Syntax Description

interface	(Optional) Displays traffic stattistics for a specified interface.
port-channel *number*	(Optional) Displays information for a specified EtherChannel. The range is from 1 to 4096.
.*subinterface-number*	(Optional) Subinterface number. Use the EtherChannel number followed by a dot (.) indicator and the subinterface number. The format is *portchannel-number***.***subinterface-number*.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the traffic statistics for all EtherChannels:

```
switch# show port-channel traffic
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
    10    Eth1/7    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
    10    Eth1/8    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
    10    Eth1/9    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
    10   Eth1/10    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
  4000    Eth1/1    0.0%    0.0%  99.64%  99.81%    0.0%    0.0%
  4000    Eth1/2    0.0%    0.0%   0.06%   0.06%    0.0%    0.0%
  4000    Eth1/3    0.0%    0.0%   0.23%   0.06%    0.0%    0.0%
  4000    Eth1/4    0.0%    0.0%   0.06%   0.06%    0.0%    0.0%
switch#
```

This example shows how to display the traffic statistics for a specific EtherChannel:

```
switch# show port-channel traffic interface port-channel 10
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
    10    Eth1/7    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
    10    Eth1/8    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
    10    Eth1/9    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
    10   Eth1/10    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for EtherChannels.
show tech-support port-channel	Displays Cisco Technical Support information about EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

show port-channel usage

To display the range of used and unused EtherChannel numbers, use the **show port-channel usage** command.

show port-channel usage

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the EtherChannel usage information:

```
switch# show port-channel usage
Total 29 port-channel numbers used
============================================
Used  :   19 , 21 , 50 , 100 , 150 , 170 - 171 , 198 - 199 , 256
          301 , 400 - 401 , 1032 - 1033 , 1111 , 1504 , 1511 , 1514 , 1516 - 1520
          1532 , 1548 , 1723 , 1905 , 1912
Unused:   1 - 18 , 20 , 22 - 49 , 51 - 99 , 101 - 149 , 151 - 169
          172 - 197 , 200 - 255 , 257 - 300 , 302 - 399 , 402 - 1031
          1034 - 1110 , 1112 - 1503 , 1505 - 1510 , 1512 - 1513 , 1515 , 1521 - 1531
          1533 - 1547 , 1549 - 1722 , 1724 - 1904 , 1906 - 1911 , 1913 - 4096
          (some numbers may be in use by SAN port channels)

switch#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for EtherChannels.
show tech-support port-channel	Displays Cisco Technical Support information about EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

show resource

To display the number of resources currently available in the system, use the **show resource** command.

show resource [*resource*]

Syntax Description

resource	Resource name, which can be one of the following: • **port-channel**—Displays the number of EtherChannels available in the system. • **vlan**—Displays the number of VLANs available in the system. • **vrf**—Displays the number of virtual routing and forwardings (VRFs) available in the system.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the resources available in the system:

```
switch# show resource

     Resource              Min       Max      Used    Unused     Avail
    -----------           -----     -----    ------  --------   -------
     vlan                 16        4094       509         0         3
     monitor-session       0           2         0         0         2
     vrf                   2        1000         2         0       998
     port-channel          0         768         2         0       766
     u4route-mem          32          32         1        31        31
     u6route-mem          16          16         1        15        15
     m4route-mem          58          58         0        58        58
     m6route-mem           8           8         0         8         8
     bundle-map            0          16         2         0        14

switch#
```

Related Commands

Command	Description
show interface port-channel	Displays information about EtherChannels.

Send comments to nx5000-docfeedback@cisco.com

show running-config

To display the contents of the currently running configuration file, use the **show running-config** command.

show running-config [**all**]

Syntax Description

all	(Optional) Displays the full operating information including default settings.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

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

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

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

```
switch# show running-config all
```

Related Commands

Command	Description
show startup-config	Displays the contents of the startup configuration file.

Send comments to nx5000-docfeedback@cisco.com

show running-config spanning-tree

To display the running configuration for the Spanning Tree Protocol (STP), use the **show running-config spanning-tree** command.

show running-config spanning-tree [**all**]

Syntax Description

all	(Optional) Displays current STP operating information including default settings.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
switch# show running-config spanning-tree
```

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

```
switch# show running-config spanning-tree all
```

Note Display output differs slightly depending on whether you are running Rapid Per VLAN Spanning Tree Plus (Rapid PVST+) or Multiple Spanning Tree (MST).

Related Commands

Command	Description
show spanning-tree	Displays information about STP.

Send comments to nx5000-docfeedback@cisco.com

show running-config vlan

To display the running configuration for a specified VLAN, use the **show running-config vlan** command.

show running-config vlan *vlan-id*

Syntax Description

vlan-id	Number of VLAN or range of VLANs. Valid numbers are from 1 to 4096.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command provides information on the specified VLAN, including private VLANs.

The display varies with your configuration. If you have configured the VLAN name, shutdown status, or suspended status, these are also displayed.

Examples

This example shows how to display the running configuration for VLAN 5:

```
switch# show running-config vlan 5
```

Related Commands

Command	Description
show vlan	Displays information about all the VLANs on the switch.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree

To display information about the Spanning Tree Protocol (STP), use the **show spanning-tree** command.

show spanning-tree [**blockedports** | **inconsistentports** | **pathcost method**]

Syntax Description

blockedports	(Optional) Displays the alternate ports blocked by STP.
inconsistentports	(Optional) Displays the ports that are in an inconsistent STP state.
pathcost method	(Optional) Displays whether short or long path cost method is used. The method differs for Rapid Per VLAN Spanning Tree Plus (Rapid PVST+) (configurable, default is short) and Multiple Spanning Tree (MST) (nonconfigurable, operational value is always long).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The STP port type displays only when you have configured the port as either an STP edge port or an STP network port. If you have not configured the STP port type, no port type displays.

Table 3-2 describes the fields that are displayed in the output of **show spanning-tree** commands.

Table 3-2 show spanning-tree Command Output Fields

Field	Definition
Role	Current port STP role. Valid values are as follows: • Desg (designated) • Root • Altn (alternate) • Back (backup)

Send comments to nx5000-docfeedback@cisco.com

Table 3-2 show spanning-tree Command Output Fields (continued)

Field	Definition
Sts	Current port STP state. Valid values are as follows: • BLK (blocking) • DIS (disabled) • LRN (learning) • FWD (forwarding)
Type	Status information. Valid values are as follows: • P2p/Shr—The interface is considered as a point-to-point (shared) interface by the spanning tree. • Edge—The port is configured as an STP edge port (either globally using the **default** command or directly on the interface) and no BPDU has been received. • Network—The port is configured as an STP network port (either globally using the **default** command or directly on the interface). • *ROOT_Inc, *LOOP_Inc, *PVID_Inc, *BA_Inc, and *TYPE_Inc—The port is in a broken state (BKN*) for an inconsistency. The broken states are Root inconsistent, Loopguard inconsistent, PVID inconsistent, Bridge Assurance inconsistent, or Type inconsistent.

Note Display output differs slightly depending on whether you are running Rapid Per VLAN Spanning Tree Plus (Rapid PVST+) or Multiple Spanning Tree (MST).

Examples

This example shows how to display spanning tree information:

```
switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    1
             Address     000d.ecb0.fdbc
             Cost        2
             Port        4096 (port-channel1)
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    61441  (priority 61440 sys-id-ext 1)
             Address     0005.9b78.6e7c
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 1         128.4096 (vPC peer-link) Network P2p
Po3              Root FWD 1         128.4098 (vPC) P2p
Po123            Desg FWD 4         128.4218 Edge P2p
Eth1/11          Desg BKN*2         128.139  P2p *TYPE_Inc
Eth1/12          Desg BKN*2         128.140  P2p *TYPE_Inc
Eth1/15          Desg BKN*2         128.143  P2p *TYPE_Inc
Eth1/16          Desg BKN*2         128.144  P2p *TYPE_Inc
Eth1/33          Desg FWD 2         128.161  Edge P2p
Eth1/35          Desg FWD 2         128.163  Edge P2p
```

Send comments to nx5000-docfeedback@cisco.com

```
Eth1/36          Desg FWD 2         128.164  Edge P2p
Eth1/38          Desg FWD 2         128.166  Edge P2p
Eth100/1/1       Desg FWD 1         128.1025 (vPC) Edge P2p
Eth100/1/2       Desg FWD 1         128.1026 (vPC) Edge P2p
Eth100/1/3       Desg FWD 1         128.1027 (vPC) Edge P2p
Eth100/1/4       Desg FWD 1         128.1028 (vPC) Edge P2p
--More--
switch#
```

This example shows how to display the blocked ports in spanning tree:

```
switch(config)# show spanning-tree blockedports

Name                 Blocked Interfaces List
-------------------- ------------------------------------
VLAN0001             Eth1/11, Eth1/12, Eth1/15, Eth1/16


Number of blocked ports (segments) in the system : 4

switch#
```

This example shows how to determine if any ports are in any STP-inconsistent state:

```
switch# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
VLAN0001             Eth1/11                Port Type Inconsistent
VLAN0001             Eth1/12                Port Type Inconsistent
VLAN0001             Eth1/15                Port Type Inconsistent
VLAN0001             Eth1/16                Port Type Inconsistent


Number of inconsistent ports (segments) in the system : 4

switch#
```

This example shows how to display the path cost method:

```
switch(config)# show spanning-tree pathcost method
Spanning tree default pathcost method used is short
switch#
```

Related Commands

Command	Description
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree active

To display Spanning Tree Protocol (STP) information on STP-active interfaces only, use the **show spanning-tree active** command.

show spanning-tree active [**brief** | **detail**]

Syntax Description

brief	(Optional) Displays a brief summary of STP interface information.
detail	(Optional) Displays a detailed summary of STP interface information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display STP information on the STP-active interfaces:

```
switch# show spanning-tree active
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree bridge

To display the status and configuration of the local Spanning Tree Protocol (STP) bridge, use the **show spanning-tree bridge** command.

show spanning-tree bridge [**address** | **brief** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]

Syntax Description

address	(Optional) Displays the MAC address for the STP local bridge.
brief	(Optional) Displays a brief summary of the status and configuration for the STP bridge.
detail	(Optional) Displays a detailed summary of the status and configuration for the STP bridge.
forward-time	(Optional) Displays the STP forward delay interval for the bridge.
hello-time	(Optional) Displays the STP hello time for the bridge.
id	(Optional) Displays the STP bridge identifier for the bridge.
max-age	(Optional) Displays the STP maximum-aging time for the bridge.
priority	(Optional) Displays the bridge priority for this bridge.
system-id	(Optional) Displays the bridge priority with the system ID extension for this bridge.
protocol	(Optional) Displays whether the Rapid Per VLAN Spanning Tree Plus (Rapid PVST+) or Multiple Spanning Tree (MST) protocol is active.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display STP information for the bridge:

```
switch# show spanning-tree bridge
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree brief

To display a brief summary of the Spanning Tree Protocol (STP) status and configuration on the switch, use the **show spanning-tree brief** command.

show spanning-tree brief [**active**]

Syntax Description

active	(Optional) Displays information about STP active interfaces only.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display a brief summary of STP information:

```
switch(config)# show spanning-tree brief

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     000d.ecb0.fc7c
             Cost        1
             Port        4495 (port-channel400)
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000d.ece7.df7c
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po19             Desg FWD 1         128.4114 Edge P2p
Po400            Root FWD 1         128.4495 (vPC peer-link) Network P2p
Eth170/1/17      Desg FWD 2         128.3857 Edge P2p
Eth171/1/7       Desg FWD 1         128.3975 (vPC) Edge P2p
Eth171/1/8       Desg FWD 1         128.3976 (vPC) Edge P2p
Eth198/1/11      Desg FWD 1         128.1291 (vPC) Edge P2p
Eth199/1/13      Desg FWD 2         128.1677 Edge P2p


VLAN0300
  Spanning tree enabled protocol rstp
  Root ID    Priority    4396
--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree detail

To display detailed information on the Spanning Tree Protocol (STP) status and configuration on the switch, use the **show spanning-tree detail** command.

show spanning-tree detail [**active**]

Syntax Description

active	(Optional) Displays information about STP active interfaces only.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
switch(config)# show spanning-tree detail
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree interface

To display information on the Spanning Tree Protocol (STP) interface status and configuration of specified interfaces, use the **show spanning-tree interface** command.

show spanning-tree interface {**ethernet** *slot*/*port* | **port-channel** *number*} [**active** [**brief** | **detail**] | **brief** [**active**] | **cost** | **detail** [**active**] | **edge** | **inconsistency** | **priority** | **rootcost** | **state**]

Syntax Description

interface	Specifies the interface. The interface can be Ethernet or EtherChannel.
ethernet *slot*/*port*	Specifies the Ethernet interface slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and number. The EtherChannel number is from 1 to 4096.
active	(Optional) Displays information about STP active interfaces only on the specified interfaces.
brief	(Optional) Displays brief summary of STP information on the specified interfaces.
detail	(Optional) Displays detailed STP information about the specified interfaces.
cost	(Optional) Displays the STP path cost for the specified interfaces.
edge	(Optional) Displays the STP-type edge port information for the specified interfaces.
inconsistency	(Optional) Displays the port STP inconsistency state for the specified interfaces.
priority	(Optional) Displays the STP port priority for the specified interfaces.
rootcost	(Optional) Displays the path cost to the root for specified interfaces.
state	(Optional) Displays the current port STP state.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The STP port type displays only when you have configured the port as either an STP edge port or an STP network port. If you have not configured the STP port type, no port type displays.

If you specify an interface that is not running STP, the switch returns an error message.

When you are running Multiple Spanning Tree (MST), this command displays the Per VLAN Spanning Tree (PVST) simulation setting.

Send comments to nx5000-docfeedback@cisco.com

Note If you are running Multiple Spanning Tree (MST), use the **show spanning-tree mst** command to show more detail on the specified interfaces.

Examples

This example shows how to display STP information on a specified interface:

```
switch(config)# show spanning-tree interface ethernet 1/3
```

This example shows how to display detailed STP information on a specified interface:

```
switch(config)# show spanning-tree interface ethernet 1/3 detail
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree mst

To display information on Multiple Spanning Tree (MST) status and configuration, use the **show spanning-tree mst** command.

show spanning-tree mst [*instance-id* [**detail** | **interface** {**ethernet** *slot*/*port* | **port-channel** *number*} [**detail**]]

show spanning-tree mst [**configuration** [**digest**]]

show spanning-tree mst [**detail** | **interface** {**ethernet** *slot*/*port* | **port-channel** *number*} [**detail**]]

Syntax Description

instance-id	(Optional) Multiple Spanning Tree (MST) instance range that you want to display. For example, 0 to 3, 5, 7 to 9.
detail	(Optional) Displays detailed Multiple Spanning Tree (MST) information.
interface	(Optional) Specifies the interface. The interface can be Ethernet or EtherChannel.
ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface and its slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface and number. The EtherChannel number is from 1 to 4096.
configuration	(Optional) Displays current Multiple Spanning Tree (MST) regional information including the VLAN-to-instance mapping of all VLANs.
digest	(Optional) Displays information about the MD5 digest.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If the switch is not running in STP Multiple Spanning Tree (MST) mode when you enter this command, it returns the following message:

```
ERROR: Switch is not in mst mode
```

Examples

This example shows how to display STP information about Multiple Spanning Tree (MST) instance information for the VLAN ports that are currently active:

```
switch# show spanning-tree mst
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display STP information about a specific Multiple Spanning Tree (MST) instance:

```
switch)# show spanning-tree mst 0
```

This example shows how to display detailed STP information about the Multiple Spanning Tree (MST) protocol:

```
switch)# show spanning-tree mst detail
```

This example shows how to display STP information about specified Multiple Spanning Tree (MST) interfaces:

```
switch)# show spanning-tree mst interface ethernet 8/2
```

This example shows how to display information about the Multiple Spanning Tree (MST) configuration:

```
switch)# show spanning-tree mst configuration
```

This example shows how to display the MD5 digest included in the current Multiple Spanning Tree (MST) configuration:

```
switch)# show spanning-tree mst configuration digest
```

See Table 3-2 on page 3-52 for descriptions of the fields that are displayed in the output of the **show spanning-tree** commands.

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree root

To display the status and configuration of the Spanning Tree Protocol (STP) root bridge, use the **show spanning-tree root** command.

show spanning-tree root [**address** | **brief** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]

Syntax Description

address	(Optional) Displays the MAC address for the STP root bridge.
brief	(Optional) Displays a brief summary of the status and configuration for the the root bridge.
cost	(Optional) Displays the path cost from the root to this bridge.
detail	(Optional) Displays detailed information on the status and configuration for the root bridge.
forward-time	(Optional) Displays the STP forward delay interval for the root bridge.
hello-time	(Optional) Displays the STP hello time for the root bridge.
id	(Optional) Displays the STP bridge identifier for the root bridge.
max-age	(Optional) Displays the STP maximum-aging time for the root bridge.
port	(Optional) Displays which port is the root port.
priority	(Optional) Displays the bridge priority for the root bridge.
system-id	(Optional) Displays the bridge identifier with the system ID extension for the root bridge.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information for the root bridge:

```
switch(config)# show spanning-tree root
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays a brief summary of STP information.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree summary

To display summary Spanning Tree Protocol (STP) information on the switch, use the **show spanning-tree summary** command.

show spanning-tree summary [**totals**]

Syntax Description

totals	(Optional) Displays totals only of STP information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The display output for this command differs when you are running Rapid Per VLAN Spanning Tree Plus (Rapid PVST+) or Multiple Spanning Tree (MST).

Examples

This example shows how to display a summary of STP information on the switch:

```
switch(config)# show spanning-tree summary
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree vlan

To display Spanning Tree Protocol (STP) information for specified VLANs, use the **show spanning-tree vlan** command.

show spanning-tree vlan {*vlan-id*} [**active** [**brief** | **detail**]]

show spanning-tree vlan {*vlan-id*} [**blockedports**]

show spanning-tree vlan {*vlan-id*} [**bridge** [**address**] | **brief** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]

show spanning-tree vlan {*vlan-id*} [**brief** [**active**]]

show spanning-tree vlan {*vlan-id*} [**detail** [**active**]]

show spanning-tree vlan {*vlan-id*} [**inconsistentports**]

show spanning-tree vlan {*vlan-id*} [**interface** {**ethernet** *slot*/*port* | **port-channel** *number*} [**active** [**brief** | **detail**]] | **brief** [**active**] | **cost** | **detail** [**active**] | **edge** | **inconsistency** | **priority** | **rootcost** | **state**]]

show spanning-tree vlan {*vlan-id*} [**root** [**address** | **brief** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]

show spanning-tree vlan {*vlan-id*} [**summary**]

Syntax Description

vlan-id	VLAN or range of VLANs that you want to display.
active	(Optional) Displays information about STP VLANs and active ports.
brief	(Optional) Displays a brief summary of STP information for the specified VLANs.
detail	(Optional) Displays detailed STP information for the specified VLANs.
blockedports	(Optional) Displays the STP alternate ports in the blocked state for the specified VLANs.
bridge	(Optional) Displays the status and configuration of the bridge for the specified VLANs.
address	(Optional) Displays the MAC address for the specified STP bridge for the specified VLANs.
forward-time	(Optional) Displays the STP forward delay interval for the bridge for the specified VLANs.
hello-time	(Optional) Displays the STP hello time for the bridge for the specified VLANs.
id	(Optional) Displays the STP bridge identifier for the specified VLANs.
max-age	(Optional) Displays the STP maximum-aging time for the specified VLANs.
priority	(Optional) Displays the STP priority for the specified VLANs.
system-id	(Optional) Displays the bridge identification with the system ID added for the specified VLANs.
protocol	(Optional) Displays which STP protocol is active on the switch.

Send comments to nx5000-docfeedback@cisco.com

inconsistentports	(Optional) Displays the ports that are in an inconsistent STP state for specified VLANs.
interface	(Optional) Specifies the interface. The interface can be Ethernet or EtherChannel.
ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface and its slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface and number. The EtherChannel number is from 1 to 4096.
cost	(Optional) Displays the STP path cost for the specified VLANs.
edge	(Optional) Displays the STP-type edge port information for the specified interface for the specified VLANs.
inconsistency	(Optional) Displays the STP port inconsistency state for the specified interface for the specified VLANs.
priority	(Optional) Displays the STP priority for the specified VLANs.
rootcost	(Optional) Displays the path cost to the root for specified interfaces for the specified VLANs.
state	(Optional) Displays the current port STP state. Valid values are blocking, disabled, learning, and forwarding.
port	(Optional) Displays information about the root port for the specified VLANs.
summary	(Optional) Displays summary STP information on the specified VLANs.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display STP information on VLAN 1:

```
switch# show spanning-tree vlan 1
```

Related Commands

Command	Description
show spanning-tree	Displays information about STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays the bridge ID, timers, and protocol for the local bridge on the switch.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show spanning-tree brief	Displays a brief summary about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays the STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about Multiple Spanning Tree (MST) STP.
show spanning-tree root	Displays the status and configuration of the root bridge for the STP instance to which this switch belongs.
show spanning-tree summary	Displays summary information about STP.

Send comments to nx5000-docfeedback@cisco.com

show startup-config

To display the contents of the currently running configuration file, use the **show startup-config** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information from the startup configuration file:

```
switch# show startup-config
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file.

Send comments to nx5000-docfeedback@cisco.com

show tech-support port-channel

To display troubleshooting information about EtherChannel interfaces, use the **show tech-support port-channel** command.

show tech-support port-channel

Syntax Description

This command has no arguments and keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The output from the **show tech-support port-channel** command is very long. To better manage this output, you can redirect the output to a file.

Examples

This example shows how to display Cisco technical support information for EtherChannel interfaces:

```
switch# show tech-support port-channel
`show port-channel internal event-history all`
Low Priority Pending queue: len(0), max len(2) [Thu Jul  8 04:05:04 2010]
High Priority Pending queue: len(0), max len(32) [Thu Jul  8 04:05:04 2010]
PCM Control Block info:
pcm_max_channels        : 4096
pcm_max_channel_in_use  : 1912
pc count                : 29
hif-pc count            : 20
Max PC Cnt              : 768
==================================================
PORT CHANNELS:

port-channel19
channel       : 19
bundle        : 65535
ifindex       : 0x16000012
admin mode    : active
oper mode     : active
fop ifindex   : 0x1fc605c0
nports        : 4
active        : 4
pre cfg       : 0
ltl:          : 0
lif:          : 0
iod:          : 43
global id     : 1
```

Send comments to nx5000-docfeedback@cisco.com

```
flag          : 0
--More--
<---output truncated--->
switch#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing method among the interfaces in the channel-group bundle.
show port-channel load-balance	Displays information on EtherChannel load balancing.

Send comments to nx5000-docfeedback@cisco.com

show udld

To display the Unidirectional Link Detection (UDLD) information for a switch, use the **show udld** command.

show udld [**ethernet** *slot*/*port* | **global** | **neighbors**]

Syntax Description

ethernet *slot*/*port*	Displays UDLD information for an Ethernet IEEE 802.3z interface. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
global	Displays the UDLD global status and configuration information on all interfaces.
neighbors	Displays information about UDLD neighbor interfaces.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Examples

This example shows how to display UDLD information for all interfaces:

```
switch# show udld

Interface Ethernet1/1
------------------------------
Port enable administrative configuration setting: device-default
Port enable operational state: enabled
Current bidirectional state: bidirectional
Current operational state:  advertisement - Single neighbor detected
Message interval: 15
Timeout interval: 5

        Entry 1
        ----------------
        Expiration time: 41
        Cache Device index: 1
        Current neighbor state: bidirectional
        Device ID: FLC12280095
        Port ID: Ethernet1/1
        Neighbor echo 1 devices: SSI130205RT
        Neighbor echo 1 port: Ethernet1/1

        Message interval: 15
        Timeout interval: 5
        CDP Device name: N5Kswitch-2(FLC12280095)


Interface Ethernet1/2
```

Send comments to nx5000-docfeedback@cisco.com

```
------------------------------
Port enable administrative configuration setting: device-default
Port enable operational state: enabled
Current bidirectional state: bidirectional
Current operational state:  advertisement - Single neighbor detected
Message interval: 15
Timeout interval: 5

        Entry 1
        ----------------
--More--
switch#
```

This example shows how to display the UDLD information for a specified interface:

```
switch# show udld ethernet 1/1

Interface Ethernet1/1
------------------------------
Port enable administrative configuration setting: device-default
Port enable operational state: enabled
Current bidirectional state: bidirectional
Current operational state:  advertisement - Single neighbor detected
Message interval: 15
Timeout interval: 5

        Entry 1
        ----------------
        Expiration time: 41
        Cache Device index: 1
        Current neighbor state: bidirectional
        Device ID: FLC12280095
        Port ID: Ethernet1/1
        Neighbor echo 1 devices: SSI130205RT
        Neighbor echo 1 port: Ethernet1/1

        Message interval: 15
        Timeout interval: 5
        CDP Device name: N5Kswitch-2(FLC12280095)

switch#
```

This example shows how to display the UDLD global status and configuration on all interfaces:

```
switch# show udld global

UDLD global configuration mode: enabled
UDLD global message interval: 15
switch#
```

This example shows how to display the UDLD neighbor interfaces:

```
switch# show udld neighbors
Port             Device Name    Device ID   Port ID         Neighbor State
--------------------------------------------------------------------------------
Ethernet1/1      FLC12280095    1           Ethernet1/1     bidirectional
Ethernet1/2      FLC12280095    1           Ethernet1/2     bidirectional
Ethernet1/3      FLC12280095    1           Ethernet1/3     bidirectional
Ethernet1/4      FLC12280095    1           Ethernet1/4     bidirectional
Ethernet1/7      JAF1346000H    1           Ethernet1/7     bidirectional
Ethernet1/8      JAF1346000H    1           Ethernet1/8     bidirectional
Ethernet1/9      JAF1346000C    1           Ethernet1/9     bidirectional
Ethernet1/10     JAF1346000C    1           Ethernet1/10    bidirectional

switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
udld (configuration mode)	Configures the UDLD protocol on the switch.
udld (Ethernet)	Configures the UDLD protocol on an Ethernet interface.

Send comments to nx5000-docfeedback@cisco.com

show vlan

To display VLAN information, use the **show vlan** command.

show vlan [**brief** | **name** {*name*} | **summary**]

Syntax Description

brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
name *name*	(Optional) Displays information about a single VLAN that is identified by the VLAN name.
summary	(Optional) Displays the number of existing VLANs on the switch.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command displays information for all VLANs, including private VLANs, on the switch.

Each access port can belong to only one VLAN. Trunk ports can be on multiple VLANs.

Note Although a port can be associated with a VLAN as an access VLAN, a native VLAN, or one of the trunk allowed ports, only access VLANs are shown under Ports in the display.

If you shut down a VLAN using the **state suspend** or the **state active** command, these values appear in the Status field:

- suspended—VLAN is suspended.
- active—VLAN is active.

If you shut down a VLAN using the **shutdown** command, these values appear in the Status field:

- act/lshut—VLAN status is active but shut down locally.
- sus/lshut—VLAN status is suspended but shut down locally.

If a VLAN is shut down internally, these values appear in the Status field:

- act/ishut—VLAN status is active but shut down internally.
- sus/ishut—VLAN status is suspended but shut down internally.

If a VLAN is shut down locally and internally, the value that is displayed in the Status field is act/ishut or sus/ishut. If a VLAN is shut down locally only, the value that is displayed in the Status field is act/lshut or sus/lshut.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to display information for all VLANs on the switch:

```
switch# show vlan
```

This example shows how to display the VLAN name, status, and associated ports only:

```
switch# show vlan brief
```

This example shows how to display the VLAN information for a specific VLAN by name:

```
switch# show vlan name test
```

This example shows how to display information about the number of VLANs configured on the switch:

```
switch# show vlan summary
```

Related Commands

Command	Description
show interface switchport	Displays information about the ports, including those in private VLANs.
show vlan private-vlan	Displays private VLAN information.

Send comments to nx5000-docfeedback@cisco.com

show vlan dot1Q tag native

To display the status of tagging on the native VLANs, use the **show vlan dot1Q tag native** command.

show vlan dot1Q tag native

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the status of 802.1Q tagging on the native VLANs:

```
switch# show vlan dot1Q tag native
vlan dot1q native tag is enabled
switch#
```

Related Commands

Command	Description
vlan dot1q tag nativet	Enables dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch.

Send comments to nx5000-docfeedback@cisco.com

show vlan id

To display information and statistics for an individual VLAN or a range of VLANs, use the **show vlan id** command.

show vlan id {*vlan-id*}

Syntax Description

vlan-id	VLAN or range of VLANs that you want to display.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to display information and statistics on an individual VLAN or a range of VLANs, including private VLANs.

Note You can also display information about individual VLANs using the **show vlan name** command.

Examples

This example shows how to display information for the individual VLAN 5:

```
switch# show vlan id 5
```

Related Commands

Command	Description
show vlan	Displays information about VLANs on the switch.

Send comments to nx5000-docfeedback@cisco.com

show vlan private-vlan

To display private VLAN information, use the **show vlan private-vlan** command.

show vlan [**id** {*vlan-id*}] **private-vlan** [**type**]

Syntax Description

id *vlan-id*	(Optional) Displays private VLAN information for the specified VLAN.
type	(Optional) Displays the private VLAN type (primary, isolated, or community).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information on all private VLANs on the switch:

```
switch(config)# show vlan private-vlan
```

This example shows how to display information for a specific private VLAN:

```
switch(config)# show vlan id 42 private-vlan
```

This example shows how to display information on the types of all private VLANs on the switch:

```
switch(config)# show vlan private-vlan type
```

This example shows how to display information on the type for the specified private VLAN:

```
switch(config)# show vlan id 42 private-vlan type
```

Related Commands

Command	Description
show interface private-vlan mapping	Displays information about the private VLAN mapping between the primary and secondary VLANs so that both VLANs share the same primary VLAN interface.
show interface switchport	Displays information about the ports, including those in private VLANs.
show vlan	Displays information about all the VLANs on the switch.

Send comments to nx5000-docfeedback@cisco.com

show vtp status

To display the VLAN Trunking Protocol (VTP) domain status information, use the **show vtp status** command.

show vtp status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable VTP on the switch by using the **feature vtp** command.

Examples

This example shows how to display the VTP domain status:

```
switch# show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
VTP Operating Mode              : Transparent
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
switch#
```

Related Commands

Command	Description
feature vtp	Enables VTP on the switch.
vtp domain	Configures the VTP domain.
vtp mode	Configures the VTP device mode.
vtp version	Configures the VTP version.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 4

Fabric Extender Commands

This chapter describes the Cisco NX-OS commands used to manage a Cisco Nexus 2000 Series Fabric Extender from a Cisco Nexus 5000 Series switch.

Send comments to nx5000-docfeedback@cisco.com

attach fex

To access the command-line interface (CLI) of a connected Fabric Extender to run diagnostic commands, use the **attach fex** command.

attach fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Usage Guidelines

Use the **attach fex** command to access the CLI on a connected Fabric Extender and performing diagnostic commands. We recommend that you use this command only following direction from Cisco technical support personnel.

Examples

This example shows how to access the CLI of a connected Fabric Extender to run diagnostic commands:

```
switch# attach fex 101
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

beacon

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

beacon

no beacon

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.
4.1(3)N1(1)	This command was deprecated, and the **locator-led** command was introduced.

Usage Guidelines

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

Examples

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

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# beacon
```

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

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no beacon
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters Fabric Extender configuration mode.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

description (fex)

To specify a description for a Fabric Extender, use the **description** command. To revert to the default description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	Description of a Fabric Extender. The default is the string FEX*xxxx* where *xxxx* is the chassis ID. For example, if the chassis ID is 123, the default description is FEX0123. The maximum length is 20 alphanumeric characters.

Command Default

None

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to specify a description for a Fabric Extender:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# description Rack16_FEX101
```

This example shows how to revert to the default description for a Fabric Extender:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no description
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters Fabric Extender configuration mode.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

fex

To create a Fabric Extender and enter fabric extender configuration mode, use the **fex** command. To delete the Fabric Extender configuration, use the **no** form of this command.

fex *chassis_ID*

no fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Usage Guidelines

You can create and configure the Fabric Extender before you connect and associate it to an interface on the parent switch. Once you associate the Fabric Extender to the switch, the configuration you created is transferred over to the Fabric Extender and applied.

Examples

This example shows how to enter Fabric Extender configuration mode:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)#
```

This example shows how to delete the Fabric Extender configuration:

```
switch(config-fex)# no fex 101
switch(config)#
```

Related Commands

Command	Description
beacon	Turns on the locator beacon LED of a Fabric Extender.
description (fex)	Specifies a description for a Fabric Extender.
fex associate	Associates a Fabric Extender to an Ethernet or EtherChannel interface.
pinning max-links	Specifies the number of statically pinned uplinks connected to a Fabric Extender.
serial	Assigns a serial number to a Fabric Extender.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.
type	Specifies the Fabric Extender card.

Send comments to nx5000-docfeedback@cisco.com

fex associate

To associate a Fabric Extender to a fabric interface, use the **fex associate** command. To disassociate the Fabric Extender, use the **no** form of this command.

fex associate *chassis_ID*

no fex associate [*chassis_ID*]

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Usage Guidelines

Before you can associate an interface on the parent switch to the Fabric Extender, you must first make the interface into a fabric interface by entering the **switchport mode fex-fabric** command.

Note On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release 4.2(1)N1(1), the **switchport mode fex-fabric** command is not supported on an Ethernet interface.

Examples

This example shows how to associate the Fabric Extender to an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/40
switch(config-if)# switchport mode fex-fabric
switch(config-if)# fex associate 101
```

This example shows how to associate the Fabric Extender to an EtherChannel interface:

```
switch# configure terminal
switch(config)# interface port-channel 4
switch(config-if)# switchport mode fex-fabric
switch(config-if)# fex associate 101
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.
switchport mode fex-fabric	Sets the interface to be an uplink port.

Send comments to nx5000-docfeedback@cisco.com

fex pinning redistribute

To redistribute the host interfaces on a Fabric Extender, use the **fex pinning redistribute** command.

fex pinning redistribute *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Usage Guidelines

When you provision the Fabric Extender using the statically pinned mode (see the *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*, the host interfaces on the Fabric Extender are pinned to the fabric interfaces in the order that they were initially configured. The next time that you reboot the Fabric Extender, the configured fabric interfaces are pinned to the host interfaces in an ascending order by the port number of the fabric interface.

Use the **fex pinning redistribute** command if you want to configure the same fixed distribution of host interfaces without restarting the Fabric Extender after your initial configuration.

Caution This command disrupts all the host interface ports of the Fabric Extender. However, the disruption is shorter than would be the case if you reboot the Fabric Extender.

Examples

This example shows how to redistribute the host interfaces on a Fabric Extender:

```
switch# fex pinning redistribute 101
switch#
```

Related Commands

Command	Description
pinning max-links	Defines the number of uplinks on a Fabric Extender.
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show interface *interface* **fex-intf**	Displays the Fabric Extender ports pinned to a specific switch interface.

Send comments to nx5000-docfeedback@cisco.com

fex queue-limit

To limit the amount of input buffer space (in bytes) allocated to each Fabric Extender port, use the **fex queue-limit** command. To disable the drop threshold and allow a Fabric Extender port to use all available buffer space, use the **no** form of this command.

fex queue-limit

no fex queue-limit

Syntax Description

This command has no arguments or keywords.

Command Default

Fabric Extender queue limit is available in the default configuration and is set on.

Command Modes

System QoS configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

By default, the drop threshold applies to each Fabric Extender port to limit the amount of buffer being allocated for each port. To restore the default queue limit of each Fabric Extender port, use the **fex queue-limit** command.

Examples

This example shows how to set the queue limit for the input buffer for each Fabric Extender port:

```
switch(config)# system qos
switch(config-sys-qos)# fex queue-limit
switch(config-sys-qos)#
```

This example shows how to restore the default queue limit for each Fabric Extender port:

```
switch(config)# system qos
switch(config-sys-qos)# no fex queue-limit
switch(config-sys-qos)#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

hardware buffer-threshold

To limit the amount of input hardware buffer usage for each Fabric Extender, use the **hardware buffer-threshold** command. To revert to the default and allow a Fabric Extender to use all available hardware buffer space, use the **no** form of this command.

hardware *fex_card_typ* **buffer-threshold** *buffer-limit*

no hardware *fex_card_typ* **buffer-threshold**

Syntax Description

fex_card_type	Fabric Extender card type. The following Fabric Extender card types are supported: • **N2148T**—Fabric Extender 48x1G 4x10G SFP+ Module • **N2224TP**—Fabric Extender 24x1G 2x10G SFP+ Module • **N2232P**—Fabric Extender 32x10G SFP+ 8x10G SFP+ Module • **N2248T**—Fabric Extender 48x1G 4x10G SFP+ Module
buffer-limit	Buffer threshold limit in bytes. The range is from 81920 to 316160.

Command Default

None

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.2(1)N2(1)	This command was introduced.

Usage Guidelines

The **buffer-threshold** keyword sets the consumption level of input buffers before an indication is sent to the egress queue to start observing the tail drop threshold. If the buffer usage is lower than the configured buffer threshold, the tail drop threshold is ignored.

Supported Cisco Nexus 2000 Series Fabric Extender

The following Cisco Nexus 2000 Series Fabric Extenders are supported on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release 4.2(1)N2(1):

- Cisco Nexus 2148T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.
- Cisco Nexus N2224TP Fabric Extender—It has two 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 24 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts. It does not support Fibre Channel over Ethernet (FCoE).

Send comments to nx5000-docfeedback@cisco.com

- Cisco Nexus 2232P Fabric Extender—It has eight 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 32 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its downlink connection to servers or hosts.
- Cisco Nexus 2248T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.

Note This command is available only on a Cisco Nexus 2148T Fabric Extender.

Examples

This example shows how to configure the hardware buffer threshold limit on a Cisco Nexus 2148T Fabric Extender:

```
switch(config)# fex 110
switch(config-fex)# hardware N2148T buffer-threshold 163840
switch(config-fex)#
```

This example shows how to remove the hardware buffer threshold configured on a Cisco Nexus 2148T Fabric Extender:

```
switch(config)# fex 110
switch(config-fex)# no hardware N2148T buffer-threshold
switch(config-fex)#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show queuing interface	Displays informtion about interface queuing parameters, including buffer threshold and queue limits.
show running-config fex	Displays the running configuration for Fabric Extenders.

Send comments to nx5000-docfeedback@cisco.com

hardware queue-limit

To control the egress queue tail drop threshold level on a Fabric Extender, use the **hardware queue-limit** command. To disable the drop threshold and allow a Fabric Extender to use all available hardware buffer space, use the **no** form of this command.

hardware *fex_card_typ* **queue-limit** [*queue-limit*]

no hardware *fex_card_typ* **queue-limit**

Syntax Description

fex_card_type	Fabric Extender card type. The following Fabric Extender card types are supported: • **N2148T**—Fabric Extender 48x1G 4x10G SFP+ Module • **N2224TP**—Fabric Extender 24x1G 2x10G SFP+ Module • **N2232P**—Fabric Extender 32x10G SFP+ 8x10G SFP+ Module • **N2248T**—Fabric Extender 48x1G 4x10G SFP+ Module
queue-limit	(Optional) Queue limit in bytes. The range is from 81920 to 652800 for a Cisco Nexus 2148T Fabric Extender and from 2560 to 652800 for all other supported Fabric Extenders.

Command Default

None

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.2(1)N2(1)	This command was introduced.

Usage Guidelines

You can use a lower queue limit value on the Fabric Extender to prevent one blocked receiver from affecting traffic being sent to other noncongested receivers ("head-of-line blocking"); however, this will increase burst absorption on the ingress traffic. A higher queue limit value provides better burst absorption and less head-of-line blocking protection.

Supported Cisco Nexus 2000 Series Fabric Extender

The following Cisco Nexus 2000 Series Fabric Extenders are supported on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release 4.2(1)N2(1):

- Cisco Nexus 2148T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.

Send comments to nx5000-docfeedback@cisco.com

- Cisco Nexus N2224TP Fabric Extender—It has two 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 24 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts. It does not support Fibre Channel over Ethernet (FCoE).
- Cisco Nexus 2232P Fabric Extender—It has eight 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 32 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its downlink connection to servers or hosts.
- Cisco Nexus 2248T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.

Examples

This example shows how to configure the hardware buffer queue limit on a Cisco Nexus 2248T Fabric Extender:

```
switch(config)# fex 110
switch(config-fex)# hardware N2248T queue-limit 327680
switch(config-fex)#
```

This example shows how to remove the hardware buffer queue limit configured on a Cisco Nexus 2248T Fabric Extender:

```
switch(config)# fex 110
switch(config-fex)# no hardware N2248T queue-limit
switch(config-fex)#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show queuing interface	Displays informtion about interface queuing parameters, including buffer threshold and queue limits.
show running-config fex	Displays the running configuration for Fabric Extenders.

Send comments to nx5000-docfeedback@cisco.com

locator-led fex

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 fex *chassis_ID*

no locator-led fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.1(3)N1(1), the locator beacon LED was toggled with the **beacon** command.

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.

Examples

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.

Send comments to nx5000-docfeedback@cisco.com

logging fex

To set the logging alert level for Fabric Extender events, use the **logging fex** command. To reset the logging level, use the **no** form of this command.

logging fex [*severity-level*]

no logging fex [*severity-level*]

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
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to set the logging alert level for Fabric Extender events:

```
switch(config)# logging fex 4
```

This example shows how to reset the logging level:

```
switch(config)# no logging fex
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

pinning max-links

To specify the number of statically pinned uplinks, use the **pinning max-links** command. To reset to the default, use the **no** form of this command.

pinning max-links *uplinks*

no pinning max-links

Syntax Description

uplinks	Number of uplinks. The range is from 1 to 8. The default is 1. This command is applicable only if the Fabric Extender is connected to its parent switch using one or more statically pinned fabric interfaces.

Command Default

The maximum uplinks is 1.

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.
4.2(1)N1(1)	The number of uplinks is extended to 8.

Usage Guidelines

Use the **pinning max-links** command when you create a number of pinned fabric interface connections to enable the parent switch to determine a distribution of host interfaces. The host interfaces are divided by the number of *uplinks* and distributed accordingly.

Caution Changing the value of *uplinks* is disruptive. All the host interfaces on the Fabric Extender are brought down and back up as the parent switch reassigns its static pinning.

Examples

This example shows how to specify the number of statically pinned uplinks for a Fabric Extender:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# pinning max-links 4
```

This example shows how to revert to the uplink count to the default for a Fabric Extender:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no pinning max-links
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
fex pinning redistribute	Redistributes the host interfaces on a Fabric Extender.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

serial

To assign a serial number to a Fabric Extender, use the **serial** command. To remove the serial number, use the **no** form of this command.

serial *serial_string*

no serial

Syntax Description

serial_string	Serial number string for the Fabric Extender. The string is alphanumeric, case sensitive, and has a maximum length of 20 characters.

Command Default

None

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Usage Guidelines

The serial number string you define with the **serial** command must match the serial number of the Fabric Extender. If you configure a serial number and then you use the **fex associate** command to associate the corresponding chassis ID to the switch, the association will succeed only if the Fabric Extender reports a matching serial number string.

Caution Configuring a serial number other than that of the given Fabric Extender will force the Fabric Extender offline.

Examples

This example shows how to specify a serial number for a Fabric Extender:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# serial Rack16_FEX101
```

This example shows how to remove a serial number from a Fabric Extender:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no serial
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
fex associate	Associates a Fabric Extender to an Ethernet or EtherChannel interface.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show diagnostic result fex

To display the results from the diagnostic tests for a Fabric Extender chassis, use the **show diagnostic result fex** command.

show diagnostic result fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display the results from the diagnostic tests for a Fabric Extender:

```
switch# show diagnostic result fex 100
FEX-100: 48x1GE/Supervisor  SerialNo   : JAF1237ABSE
Overall Diagnostic Result for FEX-100  : OK

Test results: (. = Pass, F = Fail, U = Untested)
TestPlatform:
0)              SPROM: ---------------> .
1)          MV88E6095: ---------------> .
2)                Fan: ---------------> .
3)       Power Supply: ---------------> .
4) Temperature Sensor: ---------------> .

TestForwardingPorts:
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 ------------------------------------------------------------------------
       .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

TestFabricPorts:
Fabric 1  2  3  4
Port ------------
       .  .  .  .

switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show environment fex

To display the environmental sensor status, use the **show environment fex** command.

show environment fex {**all** | *chassis_ID*} [**temperature** | **power** | **fan**]

Syntax Description

all	Displays information for all Fabric Extender chassis.
chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.
temperature	(Optional) Displays temperature sensor information.
power	(Optional) Displays power capacity and power distribution information.
fan	(Optional) Displays fan information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display the environmental sensor status for a Fabric Extender:

```
switch# show environment fex 100

Temperature Fex 100:
-----------------------------------------------------------------------
Module   Sensor     MajorThresh   MinorThres   CurTemp     Status
                    (Celsius)     (Celsius)    (Celsius)
-----------------------------------------------------------------------
1        Outlet-1   85            75           50          ok
1        Inlet-1    100           90           37          ok


Fan Fex: 100:
-----------------------------------------------------
Fan             Model                Hw         Status
-----------------------------------------------------
Chassis         N2K-C2148-FAN        --         ok
PS-1            N5K-PAC-200W         --         ok
PS-2            --                   --         absent


Power Supply Fex 100:
-------------------------------------------------------------------------------
Voltage: 12 Volts
-----------------------------------------------------
PS  Model                Power       Power     Status
                         (Watts)     (Amp)
-----------------------------------------------------
1   N5K-PAC-200W           0.00      0.00      ok
```

Send comments to nx5000-docfeedback@cisco.com

```
2   --                        --        --     --


Mod Model               Power     Power       Power     Power       Status
                        Requested Requested   Allocated Allocated
                        (Watts)   (Amp)       (Watts)   (Amp)
--- ------------------  -------   ----------  --------- ----------  ----------
1    N5K-C5110T-BF-1GE  24.00     2.00        24.00     2.00        powered-up


Power Usage Summary:
--------------------
Power Supply redundancy mode:                redundant

Total Power Capacity                              0.00 W

Power reserved for Supervisor(s)                 24.00 W
Power currently used by Modules                   0.00 W

                                                -------------
Total Power Available                            -24.00 W
                                                -------------
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show fex

To display information about a specific Fabric Extender or all attached chassis, use the **show fex** command.

show fex [*chassis_ID* [**detail**]]

Syntax Description

chassis_ID	(Optional) Fabric Extender chassis ID. The chassis ID range is from 100 to 199.
detail	(Optional) Displays a detailed listing.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display information about all attached Fabric Extender chassis:

```
switch# show fex
FEX         FEX           FEX                      FEX
Number    Description      State            Model            Serial
------------------------------------------------------------------------
100        FEX0100               Online   N5K-C5110T-BF-1GE   JAF1237ABSE
101        FEX0101               Online     N2K-C2248TP-1GE   JAF11223333
102        FEX0102               Online   N5K-C5110T-BF-1GE   JAF1241BLHQ
105        FEX0105               Online     N2K-C2232P-10GE   JAF1331AKBM
switch#
```

This example shows how to display information about a specific Fabric Extender chassis:

```
switch# show fex 101
FEX: 101 Description: FEX0101   state: Online
  FEX version: 4.2(1)N1(1) [Switch version: 4.2(1)N1(1)]
  Extender Model: N2K-C2248TP-1GE,  Extender Serial: JAF11223333
  Part No: 73-12748-01
 pinning-mode: static    Max-links: 1
  Fabric port for control traffic: Eth3/5
  Fabric interface state:
    Po5 - Interface Up. State: Active
    Eth3/5 - Interface Up. State: Active
    Eth3/6 - Interface Up. State: Active
switch#
```

This example shows how to display the detailed information about all attached Fabric Extender chassis:

```
switch# show fex detail
FEX: 100 Description: FEX0100   state: Online
  FEX version: 4.2(1)N1(1) [Switch version: 4.2(1)N1(1)]
```

Send comments to nx5000-docfeedback@cisco.com

```
  FEX Interim version: 4.2(1)N1(0.309)
  Switch Interim version: 4.2(1)N1(0.309)
  Extender Model: N5K-C5110T-BF-1GE,  Extender Serial: JAF1237ABSE
  Part No: 73-12009-02
  Card Id: 70, Mac Addr: 00:0d:ec:b1:13:02, Num Macs: 64
  Module Sw Gen: 12594  [Switch Sw Gen: 21]
  post level: complete
 pinning-mode: static    Max-links: 1
  Fabric port for control traffic: Eth3/3
  Fabric interface state:
    Po12 - Interface Up. State: Active
    Eth3/3 - Interface Up. State: Active
    Eth3/4 - Interface Up. State: Active
  Fex Port        State  Fabric Port  Primary Fabric
       Eth100/1/1    Up        Po12        Po12
       Eth100/1/2    Up        Po12        Po12
       Eth100/1/3    Up        Po12        Po12
       Eth100/1/4    Up        Po12        Po12
       Eth100/1/5    Up        Po12        Po12
       Eth100/1/6    Up        Po12        Po12
       Eth100/1/7    Up        Po12        Po12
       Eth100/1/8    Up        Po12        Po12
       Eth100/1/9    Up        Po12        Po12
      Eth100/1/10    Up        Po12        Po12
      Eth100/1/11    Up        Po12        Po12
      Eth100/1/12    Up        Po12        Po12
      Eth100/1/13    Up        Po12        Po12
      Eth100/1/14    Up        Po12        Po12
      Eth100/1/15    Up        Po12        Po12
      Eth100/1/16    Up        Po12        Po12
      Eth100/1/17    Up        Po12        Po12
      Eth100/1/18    Up        Po12        Po12
      Eth100/1/19    Up        Po12        Po12
      Eth100/1/20    Up        Po12        Po12
      Eth100/1/21    Up        Po12        Po12
      Eth100/1/22    Up        Po12        Po12
      Eth100/1/23    Up        Po12        Po12
--More--
switch#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.

Send comments to nx5000-docfeedback@cisco.com

show fex detail

To display detailed information about a specific Fabric Extender or all attached chassis, use the **show fex detail** command.

show fex detail

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display detailed information about all attached Fabric Extender chassis:

```
switch# show fex detail
FEX: 100 Description: FEX0100   state: Online
  FEX version: 4.2(1)N1(1) [Switch version: 4.2(1)N1(1)]
  FEX Interim version: 4.2(1)N1(0.326)
  Switch Interim version: 4.2(1)N1(0.326)
  Extender Model: N5K-C5110T-BF-1GE,  Extender Serial: JAF1237ABSE
  Part No: 73-12009-02
  Card Id: 70, Mac Addr: 00:0d:ec:b1:13:02, Num Macs: 64
  Module Sw Gen: 12594  [Switch Sw Gen: 21]
  post level: complete
 pinning-mode: static    Max-links: 1
  Fabric port for control traffic: Eth3/4
  Fabric interface state:
    Po12 - Interface Up. State: Active
    Eth3/3 - Interface Up. State: Active
    Eth3/4 - Interface Up. State: Active
  Fex Port        State  Fabric Port  Primary Fabric
       Eth100/1/1    Up        Po12        Po12
       Eth100/1/2    Up        Po12        Po12
       Eth100/1/3    Up        Po12        Po12
       Eth100/1/4    Up        Po12        Po12
       Eth100/1/5    Up        Po12        Po12
       Eth100/1/6    Up        Po12        Po12
       Eth100/1/7    Up        Po12        Po12
       Eth100/1/8    Up        Po12        Po12
       Eth100/1/9    Up        Po12        Po12
      Eth100/1/10    Up        Po12        Po12
      Eth100/1/11    Up        Po12        Po12
      Eth100/1/12    Up        Po12        Po12
      Eth100/1/13    Up        Po12        Po12
      Eth100/1/14    Up        Po12        Po12
      Eth100/1/15    Up        Po12        Po12
      Eth100/1/16    Up        Po12        Po12
```

Send comments to nx5000-docfeedback@cisco.com

```
      Eth100/1/17    Up         Po12        Po12
      Eth100/1/18    Up         Po12        Po12
      Eth100/1/19    Up         Po12        Po12
      Eth100/1/20    Up         Po12        Po12
      Eth100/1/21    Up         Po12        Po12
      Eth100/1/22    Up         Po12        Po12
      Eth100/1/23    Up         Po12        Po12
      Eth100/1/24    Up         Po12        Po12
      Eth100/1/25    Up         Po12        Po12
      Eth100/1/26    Up         Po12        Po12
      Eth100/1/27    Up         Po12        Po12
      Eth100/1/28    Up         Po12        Po12
      Eth100/1/29    Up         Po12        Po12
      Eth100/1/30    Up         Po12        Po12
      Eth100/1/31    Up         Po12        Po12
      Eth100/1/32    Up         Po12        Po12
      Eth100/1/33  Down         Po12        Po12
      Eth100/1/34  Down         Po12        Po12
      Eth100/1/35  Down         Po12        Po12
      Eth100/1/36  Down         Po12        Po12
      Eth100/1/37  Down         Po12        Po12
      Eth100/1/38  Down         Po12        Po12
      Eth100/1/39  Down         Po12        Po12
      Eth100/1/40    Up         Po12        Po12
      Eth100/1/41    Up         Po12        Po12
      Eth100/1/42    Up         Po12        Po12
      Eth100/1/43    Up         Po12        Po12
      Eth100/1/44    Up         Po12        Po12
      Eth100/1/45    Up         Po12        Po12
      Eth100/1/46    Up         Po12        Po12
      Eth100/1/47    Up         Po12        Po12
      Eth100/1/48    Up         Po12        Po12
Logs:
04/16/2010 05:05:23.441707: Module register received
04/16/2010 05:05:23.442886: Registration response sent
04/16/2010 05:05:23.551846: Module Online Sequence
04/16/2010 05:05:56.520856: Module Online
04/16/2010 05:29:38.526605: Deleting route to FEX
04/16/2010 05:29:38.536055: Module disconnected
04/16/2010 05:29:38.537686: Offlining Module
04/16/2010 05:29:38.538260: Module Offline Sequence
04/16/2010 05:29:53.646254: Module Offline
04/16/2010 05:29:54.178401: Deleting route to FEX
04/16/2010 05:29:54.184092: Module disconnected
04/16/2010 05:29:54.186230: Offlining Module
04/16/2010 05:31:13.784346: Module register received
04/16/2010 05:31:13.785410: Registration response sent
04/16/2010 05:31:15.676906: Module Online Sequence
04/16/2010 05:31:50.492714: Module Online
04/16/2010 05:32:18.388033: Deleting route to FEX
04/16/2010 05:32:18.393579: Module disconnected
04/16/2010 05:32:18.394845: Offlining Module
04/16/2010 05:32:18.395412: Module Offline Sequence
04/16/2010 05:32:30.336790: Module Offline
04/16/2010 05:32:30.683558: Deleting route to FEX
04/16/2010 05:32:30.690042: Module disconnected
04/16/2010 05:32:30.692101: Offlining Module
04/16/2010 05:33:42.781911: Module register received
04/16/2010 05:33:42.783432: Registration response sent
04/16/2010 05:33:52.542824: Module Online Sequence
04/16/2010 05:34:33.483417: Module Online
<---output truncated--->
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show fex transceiver

To display information about the transceiver connecting a Fabric Extender to the Cisco Nexus 5000 Series switch, use the **show fex transceiver** command.

show fex *chassis_ID* **transceiver** [**calibration** | **detail**]

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.
calibration	(Optional) Displays detailed calibration information about the transceiver.
detail	(Optional) Displays detailed diagnostic information about the transceiver.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display information about the transceiver that connects a Fabric Extender to the Cisco Nexus 5000 Series switch:

```
switch# show fex 101 transceiver

Fex Uplink: 1
Fabric Port: Ethernet3/5
    sfp is present
    name is CISCO-AVAGO
    part number is SFBR-7700SDZ
    revision is B4
    serial number is AGD113921ZR
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125mm fiber is 82 m(s)
    Link length supported for 62.5/125mm fiber is 26 m(s)
    cisco id is --
    cisco extended id number is 4


Fex Uplink: 2
Fabric Port: Ethernet3/6
    sfp is present
    name is CISCO-AVAGO
    part number is SFBR-7700SDZ
    revision is B4
    serial number is AGD113422LS
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125mm fiber is 82 m(s)
    Link length supported for 62.5/125mm fiber is 26 m(s)
    cisco id is --
    cisco extended id number is 4
```

Send comments to nx5000-docfeedback@cisco.com

```
Fex Uplink: 3
Fabric Port: --
    sfp is present
    name is CISCO-AVAGO
    part number is SFBR-7700SDZ
    revision is B4
    serial number is AGD11392258
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125mm fiber is 82 m(s)
    Link length supported for 62.5/125mm fiber is 26 m(s)
--More--
switch#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.

Send comments to nx5000-docfeedback@cisco.com

show fex version

To display the version information about a Fabric Extender, use the **show fex version** command.

show fex *chassis_ID* **version**

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display the version information about a Fabric Extender:

```
switch# show fex 101 version
Software
  Bootloader version:           0.2
  System boot mode:             primary
  System image version:         4.2(1)N1(1) [build 4.2(1)N1(0.309)]

Hardware
  Module:                       Fabric Extender 48x1GE + 4x10G Module
  CPU:                          Motorola, e300c4
  Serial number:                JAF11223333
  Bootflash:                    locked

Kernel uptime is 0 day(s), 3 hour(s), 53 minutes(s), 43 second(s)

Last reset at Wed Mar 31 06:28:41 2010
  Reason: Kernel Reboot
  Service: Reload new image
switch#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.

Send comments to nx5000-docfeedback@cisco.com

show interface fex-fabric

To display all Fabric Extender fabric interfaces, use the **show interface fex-fabric** command.

show interface fex-fabric

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display all Fabric Extender fabric interfaces:

```
switch# show interface fex-fabric
Fabric      Fabric       Fex                FEX
Fex  Port      Port State    Uplink    Model         Serial
--------------------------------------------------------------
105    Eth1/5        Active     5    N2K-C2232P-10GE  JAF1331AKBM
105    Eth1/6        Active     6    N2K-C2232P-10GE  JAF1331AKBM
105    Eth1/7        Active     8    N2K-C2232P-10GE  JAF1331AKBM
105    Eth1/8        Active     7    N2K-C2232P-10GE  JAF1331AKBM
102   Eth1/17        Active     1    N5K-C5110T-BF-1GE  JAF1241BLHQ
102   Eth1/18    Configured     0
102   Eth1/19        Active     3    N5K-C5110T-BF-1GE  JAF1241BLHQ
102   Eth1/20        Active     4    N5K-C5110T-BF-1GE  JAF1241BLHQ
100    Eth3/3        Active     1    N5K-C5110T-BF-1GE  JAF1237ABSE
100    Eth3/4        Active     2    N5K-C5110T-BF-1GE  JAF1237ABSE
101    Eth3/5        Active     1    N2K-C2248TP-1GE  JAF11223333
101    Eth3/6        Active     2    N2K-C2248TP-1GE  JAF11223333
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show interface fex-intf

To display the host interfaces pinned to a fabric interface, use the **show interface fex-intf** command.

show interface *interface* **fex-intf**

Syntax Description

interface	Ethernet or EtherChannel interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display the host interfaces pinned to an Ethernet fabric interface on the parent switch:

```
switch# show interface ethernet 1/1 fex-intf
```

This example shows how to display the host interfaces pinned to an EtherChannel fabric interface on the parent switch:

```
switch# show interface port-channel 1 fex-intf
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show interface transceiver fex-fabric

To display information about all transceivers connected to fabric interfaces, use the **show interface transceiver fex-fabric** command.

show interface transceiver fex-fabric [**calibration** | **detail**]

Syntax Description

calibration	(Optional) Displays detailed calibration information about the transceiver.
detail	(Optional) Displays detailed diagnostic information about the transceiver.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to display information about all transceivers that connect to fabric interfaces:

```
switch# show interface transceiver fex-fabric
Ethernet1/5
    sfp is present
    name is CISCO-MOLEX INC
    part number is 74752-9025
    revision is A
    serial number is MOC12302468
    nominal bitrate is 12000 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4

Ethernet1/6
    sfp is present
    name is CISCO-MOLEX INC
    part number is 74752-9025
    revision is A
    serial number is MOC12260214
    nominal bitrate is 12000 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4

Ethernet1/7
    sfp is present
    name is CISCO-MOLEX INC
    part number is 74752-9025
    revision is A
    serial number is MOC12301888
```

Send comments to nx5000-docfeedback@cisco.com

```
    nominal bitrate is 12000 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4

Ethernet1/8
    sfp is present
    name is CISCO-MOLEX INC
--More--
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show inventory fex

To display the physical inventory of a Fabric Extender, such as the name, description, and volume ID, use the **show inventory fex** command.

show inventory fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the physical inventory of a specific Fabric Extender chassis:

```
switch# show inventory fex 100
NAME: "FEX 100 CHASSIS", DESCR: "N5K-C5110T-BF-1GE  CHASSIS"
PID: N5K-C5110T-BF-1GE , VID: V01 , SN: JAF1237ABSE

NAME: "FEX 100 Module 1", DESCR: "Fabric Extender Module: 48x1GE, 4X10GE Supervi
sor"
PID: N5K-C5110T-BF-1GE , VID: V00 , SN: JAF1237ABSE

NAME: "FEX 100 Fan 1", DESCR: "Fabric Extender Fan module"
PID: N2K-C2148-FAN     , VID: N/A , SN: N/A

NAME: "FEX 100 Power Supply 1", DESCR: "Fabric Extender AC power supply"
PID: N5K-PAC-200W      , VID: 00V0, SN: PAC12473L17

switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show locator-led

To display the status of the locator LED in a Fabric Extender, use the **show locator-led** command.

show locator-led status

Syntax Description

status	Displays the status of the locator LED in a Fabric Extender module.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the **locator-led** command to toggle the locator LED of a Fabric Extender.

Examples

This example shows how to display the modules that have the locator LED set to off or on:

```
switch# show locator-led status
Component        Locator LED Status
---------------------------------
FEX 100          off
FEX 101          off
FEX 102          off
FEX 103          off
FEX 105          off
switch#
```

Related Commands

Command	Description
locator-led	Turns on the locator LED of a Fabric Extender chassis.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show module fex

To display the module information for a Fabric Extender, use the **show module fex** command.

show module fex [**all** | *chassis_ID*]

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.
all	Displays information about all Fabric Extender modules.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the module information of Fabric Extenders:

```
switch# show module fex all
FEX Mod Ports Card Type                          Model              Status.
--- --- ----- -------------------------------- ------------------ -----------
100 1   48    Fabric Extender 48x1GE Module      N5K-C5110T-BF-1GE  present
101 1   48    Fabric Extender 48x1GE + 4x10G Mod N2K-C2248TP-1GE    present
102 1   48    Fabric Extender 48x1GE Module      N5K-C5110T-BF-1GE  present
105 1   32    Fabric Extender 32x10GE + 8x10G Mo N2K-C2232P-10GE    present

FEX Mod Sw              Hw      World-Wide-Name(s) (WWN)
--- --- --------------  ------  ---------------------------------------------
100 1   4.2(1)N1(1)     0.0     --
101 1   4.2(1)N1(1)     0.103   --
102 1   4.2(1)N1(1)     0.2     --
105 1   4.2(1)N1(1)     1.0     --

FEX Mod  MAC-Address(es)                         Serial-Num
--- ---  ------------------------------------  ----------
100 1    000d.ecb1.1300 to 000d.ecb1.132f        JAF1237ABSE
101 1    0022.bdd1.3cc0 to 0022.bdd1.3cef        JAF11223333
102 1    000d.ecb1.25c0 to 000d.ecb1.25ef        JAF1241BLHQ
105 1    000d.ecca.6f40 to 000d.ecca.6f5f        JAF1331AKBM
switch#
```

This commands shows how to display the module information for a specific Fabric Extender:

```
switch# show module fex 100
FEX Mod Ports Card Type                          Model              Status.
--- --- ----- -------------------------------- ------------------ -----------
100 1   48    Fabric Extender 48x1GE Module      N5K-C5110T-BF-1GE  present

FEX Mod Sw              Hw      World-Wide-Name(s) (WWN)
--- --- --------------  ------  ---------------------------------------------
```

Send comments to nx5000-docfeedback@cisco.com

```
100 1   4.2(1)N1(1)     0.0     --

FEX Mod  MAC-Address(es)                         Serial-Num
--- ---  ------------------------------------  ----------
100 1    000d.ecb1.1300 to 000d.ecb1.132f        JAF1237ABSE
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show queuing interface

To display the queuing information of interfaces, use the **show queuing interface** command.

show queuing interface [**ethernet** *slot-chassis-no*/*port-slot-no*/*port-no*]

Syntax Description

ethernet	(Optional) Specifies that queuing information be displayed for an Ethernet interface or a Fabric Extender.
slot-chassis-no	Slot number of the Ethernet interface or chassis ID of the Fabric Extender. The range is from 1 to 255.
port-slot-no	Port number of the Ethernet interface or the remote slot ID of the Fabric Extender. The range is from 1 to 128.
port-no	Port number of the Fabric Extender. The range is from 1 to 48.

Command Default

Displays the queuing information for all interfaces.

Command Modes

EXEC mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the queuing information, including the buffer threshold and queue limit values, of a specified interface on a switch that runs Cisco NX-OS 4.2(1)N2(1):

```
switch# show queuing interface eth101/1/1
Ethernet101/1/1 queuing information:
  Input buffer allocation:
  Qos-group: 0  3  4  (shared)
  frh: 3
  drop-type: drop
  cos: 0 2 3 4 6 7
  xon       xoff      buffer-size
  ---------+---------+-----------
  11520     21760     44800

  Qos-group: 2
  frh: 2
  drop-type: no-drop
  cos: 1 5
  xon       xoff      buffer-size
  ---------+---------+-----------
  12800     23040     46080

  Queueing:
  queue    qos-group    cos            priority  bandwidth mtu
  --------+------------+--------------+---------+---------+----
  3        0 3 4        0 2 3 4 6       WRR        99      9280
  2        2            1 5             WRR         1      9280
```

Send comments to nx5000-docfeedback@cisco.com

```
  Buffer threshold: 163840 bytes
  Queue limit: 327680 bytes

  Queue Statistics:
  queue  rx
  ------+---------------
  3      38557
  2      0

  Port Statistics:
  tx queue drop
  ---------------
  26374

  Priority-flow-control enabled: no
  Flow-control status:
  cos     qos-group   rx pause  tx pause  masked rx pause
  -------+-----------+---------+---------+---------------
  0              0    xon       xon       xon
  1              2    xon       xon       xon
  2              3    xon       xon       xon
  3              0    xon       xon       xon
  4              3    xon       xon       xon
  5              2    xon       xon       xon
  6              0    xon       xon       xon
  7            n/a    xon       xon       xon
switch#
```

Table 4-1 describes the significant fields shown in the display.

Table 4-1 show queuing interface Field Descriptions

Field	Description
Ethernet ...	Ethernet interface information.
qoS-group	Information about QoS groups configured on the switch.
sched-type	Type of schedule.
WRR	Weighted round robin(WRR). Queue eight for scheduling.
Priority	Priority of the queue.
q-size	Queue size.
drop-type	Queue drop type can be either drop or no-drop.
MTU	Maximum transmit unit (MTU) for the queue.
Xon	Transmission on at this threshold.
Xoff	Transmission off at this threshold.
Buffer threshold	Buffer threshold value for an interface.
Queue limit	Queue limit value for an interface.

Related Commands

Command	Description
hardware buffer-threshold	Configures the hardware buffer threshold.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
hardware queue-limit	Configures the hardware queue limit.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show running-config fex

To display the running configuration for Fabric Extenders (FEXs), use the **show running-config fex** command.

show running-config fex [**all**]

Syntax Description

all	(Optional) Displays FEX information including default settings.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N2(1)	This command was introduced.

Examples

This example shows how to display information on the running FEX configuration, including the buffer threshold value and queue limit:

```
switch# show running-config fex

!Command: show running-config fex
!Time: Mon Jul 19 07:56:21 2010

version 4.2(1)N2(1)
feature fex

fex 100
  pinning max-links 1
  description "RedwoodFex100"
fex 101
  pinning max-links 1
  description "FEX0101"
fex 150
  pinning max-links 1
  description "PortolaFex150"
fex 151
  pinning max-links 1
  description "PortolaFex151"
fex 160
  pinning max-links 1
  description "FEX0160"
fex 198
  hardware N2232P queue-limit 50000
  pinning max-links 1
  description "WoodsideFex198"
fex 199
  hardware N2232P queue-limit 20000
  no hardware N2248T queue-limit
  hardware N2148T buffer-threshold 163840
```

Send comments to nx5000-docfeedback@cisco.com

```
  pinning max-links 1
  description "WoodsideFex199"

interface port-channel100
  fex associate 100

interface port-channel150
--More--
switch#
```

Related Commands

Command	Description
hardware buffer-threshold	Configures the hardware buffer threshold.
hardware queue-limit	Configures the hardware queue limit.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show sprom fex

To display information about the SPROM, use the **show sprom fex** command.

show sprom fex {**all** | *chassis_ID* {**all** | **backplane** | **powersupply** *module_no*}}

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.
all	Displays all SPROM content for a specific Fabric Extender.
backplane	Displays the backplane SPROM content for a specific Fabric Extender.
powersupply	Displays the power supply SPROM content for a specific Fabric Extender.
module_no	Power supply module number for a specific Fabric Extender. The range is from 1 to 2.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display all SPROM content for a specific Fabric Extender:

```
switch# show sprom fex 100 all
DISPLAY FEX 100 SUP sprom contents
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x18c9
 EEPROM Size     : 65535
 Block Count     : 3
 FRU Major Type  : 0x6003
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-C5110T-BF-1GE
 Serial Number   : JAF1237ABSE
 Part Number     : 73-12009-02
 Part Revision   : 00
 Mfg Deviation   : 0
 H/W Version     : 0.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.12.3.1.9.72.5.0
 Power Consump   : -200
 RMA Code        : 0-0-0-0
 CLEI Code       : 00000000000
 VID             : V00
Supervisor Module specific block:
```

Send comments to nx5000-docfeedback@cisco.com

```
 Block Signature : 0x6002
 Block Version   : 2
 Block Length    : 103
 Block Checksum  : 0x2648
 Feature Bits    : 0x0
 HW Changes Bits : 0x2
Card Index      : 11011
 MAC Addresses   : 00-00-00-00-00-00
 Number of MACs  : 0
 Number of EPLD  : 0
 Port Type-Num   : 2-52
 Sensor #1       : 85,75
 Sensor #2       : 100,90
 Sensor #3       : 100,90
 Sensor #4       : 100,90
 Sensor #5       : 100,90
 Sensor #6       : 100,90
 Sensor #7       : 100,90
 Sensor #8       : 100,90
 Max Connector Power: 1000
 Cooling Requirement: 300
 Ambient Temperature: 40

DISPLAY FEX 100 backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x195d
 EEPROM Size     : 65535
 Block Count     : 5
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-C5110T-BF-1GE
Serial Number   : JAF1237ABSE
 Part Number     : 73-12009-02
 Part Revision   : 00
 Mfg Deviation   : 0
 H/W Version     : 0.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.12.3.1.3.719.0.0
 Power Consump   : -800
 RMA Code        : 0-0-0-0
 CLEI Code       : 00000000
 VID             : V01
Chassis specific block:
 Block Signature : 0x6001
 Block Version   : 3
 Block Length    : 39
 Block Checksum  : 0x28a
 Feature Bits    : 0x0
 HW Changes Bits : 0x2
 Stackmib OID    : 0
 MAC Addresses   : 00-0d-ec-b1-13-00
 Number of MACs  : 64
 OEM Enterprise  : 0
 OEM MIB Offset  : 0
 MAX Connector Power: 0
WWN software-module specific block:
 Block Signature : 0x6005
 Block Version   : 1
 Block Length    : 0
```

```
 Block Checksum  : 0x66
wwn usage bits:
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00
License software-module specific block:
 Block Signature : 0x6006
 Block Version   : 1
 Block Length    : 16
 Block Checksum  : 0x77
lic usage bits:
 00 00 00 00 00 00 00 00

DISPLAY FEX 100 power-supply 1 sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 124
 Block Checksum  : 0x15fc
 EEPROM Size     : 124
 Block Count     : 1
 FRU Major Type  : 0xab01
 FRU Minor Type  : 0x1
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-PAC-200W
 Serial Number   : PAC12473L17
 Part Number     : 341-0335-01
 Part Revision   : 01
 CLEI Code       : COUPADSBAA
 VID             : 00V0
 snmpOID         : 0.0.0.0.0.0.0.0
 H/W Version     : 0.1
 Current         : 1667
RMA Code        : 0-0-0-0
switch#
```

Send comments to nx5000-docfeedback@cisco.com

This command shows how to display the power supply SPROM contents for a specific Fabric Extender:

```
switch# show sprom fex 100 powersupply 1
DISPLAY FEX 100 power-supply 1 sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 124
 Block Checksum  : 0x15fc
 EEPROM Size     : 124
 Block Count     : 1
 FRU Major Type  : 0xab01
 FRU Minor Type  : 0x1
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-PAC-200W
 Serial Number   : PAC12473L17
 Part Number     : 341-0335-01
 Part Revision   : 01
 CLEI Code       : COUPADSBAA
 VID             : 00V0
 snmpOID         : 0.0.0.0.0.0.0.0
 H/W Version     : 0.1
 Current         : 1667
 RMA Code        : 0-0-0-0
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show system reset-reason fex

To display the reason for the last reset of the Fabric Extender, use the **show system reset-reason fex** command.

show system reset-reason fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the last reset reason for a specific Fabric Extender:

```
switch# show system reset-reason fex 100
----- reset reason for FEX 100 ---

1) At 430815 usecs after Fri Apr 16 04:27:04 2010
    Reset Reason: Reset Requested by CLI command reload (9)
    Service (Additional Info): Reload requested by supervisor
    Image Version: 4.2(1)N1(1)

2) At 505550 usecs after Fri Apr 16 03:39:50 2010
    Reset Reason: Reset due to upgrade (88)
    Service (Additional Info): Reset due to upgrade
    Image Version: 4.2(1u)N1(1u)

3) At 607267 usecs after Fri Apr 16 02:50:10 2010
    Reset Reason: Reset due to upgrade (88)
    Service (Additional Info): Reset due to upgrade
    Image Version: 4.2(1)N1(1)

4) At 857790 usecs after Fri Apr 16 02:00:22 2010
    Reset Reason: Reset due to upgrade (88)
    Service (Additional Info): Reset due to upgrade
    Image Version: 4.2(1u)N1(1u)

switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

show version fex

To display the software version information about a Fabric Extender, use the **show version fex** command.

show version fex *chassis_ID*

Syntax Description

chassis_ID	Fabric Extender chassis ID. The chassis ID range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the software version of a Fabric Extender:

```
switch# show version fex 100
Software
  Bootloader version:           1.12
  System boot mode:             primary
  System image version:         4.2(1)N2(1) [build 4.2(1)N2(1)]

Hardware
  Module:                       Fabric Extender 48x1GE Module
  CPU:                          Motorola, e300c1
  Serial number:                JAF1302ABDP
  Bootflash:                    locked

Kernel uptime is 0 day(s), 9 hour(s), 9 minutes(s), 16 second(s)

Last reset at Fri Jul 02 04:27:04 2010
  Reason: Reset Requested by CLI command reload
  Service: Reload requested by supervisor
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

switchport mode fex-fabric

To set the interface type to be an uplink port for a Fabric Extender, use the **switchport mode fex-fabric** command.

switchport mode fex-fabric

no switchport mode fex-fabric

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N2(1)	This command was introduced.

Examples

This example shows how to set an Ethernet interface to be an uplink port for a Fabric Extender:

```
switch# configure terminal
switch(config)# interface ethernet 1/40
switch(config-if)# switchport mode fex-fabric
```

This example shows how to set an EtherChannel interface to be an uplink port for a Fabric Extender:

```
switch# configure terminal
switch(config)# interface port-channel 4
switch(config-if)# switchport mode fex-fabric
```

Related Commands

Command	Description
fex associate	Associates a Fabric Extender to an Ethernet or EtherChannel interface.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

type

To set the Fabric Extender card type to a specific card, use the **type** command. To revert to the default FEX card, use the **no** form of this command.

type *fex_card_type*

no type

Syntax Description

fex_card_type	Fabric Extender card type. The following Fabric Extender card types are supported: • **N2148T**—Fabric Extender 48x1G 4x10G SFP+ Module • **N2224TP**—Fabric Extender 24x1G 2x10G SFP+ Module • **N2232P**—Fabric Extender 32x10G SFP+ 8x10G SFP+ Module • **N2248T**—Fabric Extender 48x1G 4x10G SFP+ Module

Command Default

None

Command Modes

Fabric extender configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

The following Cisco Nexus 2000 Series Fabric Extenders are supported on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release 4.2(1)N2(1):

- Cisco Nexus 2148T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.
- Cisco Nexus N2224TP Fabric Extender—It has two 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 24 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts. It does not support Fibre Channel over Ethernet (FCoE).
- Cisco Nexus 2232P Fabric Extender—It has eight 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 32 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its downlink connection to servers or hosts.
- Cisco Nexus 2248T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to configure the Fabric Extender card:

```
switch(config)# fex 100
switch(config-fex)# type N2148T
switch(config-fex)#
```

Related Commands

Command	Description
fex	Creates a Fabric Extender and enters fabric extender configuration mode.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 5

Quality of Service Commands

This chapter describes the Cisco NX-OS quality of service (QoS) commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

bandwidth (QoS)

To allocate a minimum percentage of the interface bandwidth to a queue and configure the bandwidth on both ingress and egress queues, use the **bandwidth** command. To remove a bandwidth configuration, use the **no** form of this command.

bandwidth percent *percent*

no bandwidth percent *percent*

Syntax Description

percent	Specifies the percentage of bandwidth of the underlying link rate.
percent	Percent value in the range from 1 to 100.

Command Default

Default bandwidth rate is kbps.

Command Modes

Policy map type queuing class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to set the bandwidth remaining for the specified queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# bandwidth remaining percent 25
switch(config-pmap-c-que)#
```

This example shows how to remove the bandwidth remaining for the specified queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# no bandwidth remaining percent 25
switch(config-pmap-c-que)#
```

Related Commands

Command	Description
show class-map	Displays class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

class (policy map type qos)

To add a reference to an existing qos class map in a policy map and enter the class mode, use the **class** command. To remove a class from the policy map, use the **no** form of this command.

class [**type qos**] {*class-map-name* | **class-default**}

no class {*class-map-name* | **class-default**}

Syntax Description

type qos	(Optional) Specifies the component type, which is qos for this class. By default, the type is qos.
class-default	Specifies the reserved class name that matches all traffic not classified in other classes in a policy map.
class-map-name	Reference to a class map. The class map name can be a maximum of 40 characters.

Command Default

None

Command Modes

Policy map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

Examples

This example shows how to add a reference to a qos class map at the end of a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)#
```

This example shows how to add a reference to the class-default qos class map in a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class class-default
switch(config-pmap-c-qos)#
```

This example shows how to remove a class map reference in a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# no class traffic_class1
switch(config-pmap-qos)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show class-map type qos	Displays type qos class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

class type network-qos

To add a reference to an existing network QoS class map in a policy map and enter the class mode, use the **class type network-qos** command. To remove a class from the policy map, use the **no** form of this command.

class type network-qos *class-map-name*

no class type network-qos *class-map-name*

Syntax Description

class-map-name	Reference to a network QoS class map.

Command Default

None

Command Modes

Policy map type network-qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

Examples

This example shows how to add a reference to a class map in a type network-qos policy map:

```
switch(config)# policy-map type network-qos nqos_policy
switch(config-pmap-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-pmap-nq-c)#
```

This example shows how to remove a class map reference in a type network-qos policy map:

```
switch(config)# policy-map type network-qos nqos_policy
switch(config-pmap-pmap-nq)# no class type network-qos nqos_class
switch(config-pmap-pmap-nq)#
```

Related Commands

Command	Description
show class-map type network-qos	Displays type network-qos class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

class type queuing

To add a reference to an existing queuing class map in a policy map and enter the class mode, use the **class type queuing** command. To remove a class from the policy map, use the **no** form of this command.

class type queuing *class-map-name*

no class type queuing *class-map-name*

Syntax Description

class-map-name	Reference to a system-defined queuing class map.

Command Default

None

Command Modes

Policy map type queuing configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

Examples

This example shows how to add a reference to a class map in a type queuing policy map:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-q3
switch(config-pmap-c-que)#
```

This example shows how to remove a class map reference in a type queuing policy map:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# no class type queuing 1p7q4t-out-q3
switch(config-pmap-que)#
```

Related Commands

Command	Description
show class-map type queuing	Displays the type queuing class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

class-map

To create or modify a class map and enter the class-map configuration mode, use the **class-map** command. To remove a class map, use the **no** form of this command.

class-map {[**type qos**] | **type queuing**} *class-map-name*

no class-map {[**type qos**] | **type queuing**} *class-map-name*

Syntax Description

type qos	(Optional) Specifies the component type qos for the class map. By default, the class map type is qos.
queuing	Specifies the component type queuing for the class map.
class-map-name	Name assigned to the QoS class map, or a system-defined queuing class map name. The name class-default is reserved.

Command Default

type—qos

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.1(3)N1(1)	The **type** {**qos**	**network-qos**	**queuing**} keyword was added.

Usage Guidelines

You can define a class map for each class of traffic to be used in QoS policies.

If the packet matches any of the criteria configured for this class map with the **match** command, then this class map is applied to the packet. Class maps of type queuing support only this option.

If you modify the queuing type class maps, the configuration for all ports of the specified port type on all virtual device contexts (VDCs) also changes.

You cannot delete the system-defined queuing class map names.

Examples

This example shows how to create or modify a class map:

```
switch(config)# class-map my_class1
switch(config-cmap)#
```

This example shows how to remove a class map:

```
switch(config)# no class-map my_class1
```

This example shows how to modify a queuing class map:

```
switch(config)# class-map type queuing match-any 2q4t-in-q1
switch(config-cmap-que)#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to create or modify a qos class map:

```
switch(config)# class-map my_class1
switch(config-cmap-qos)#
```

This example shows how to remove a qos class map:

```
switch(config-cmap-qos)# no class-map my_class1
switch(config)#
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map.
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

class-map type network-qos

To create or modify a class map that defines a network QoS class of traffic and enter the class-map configuration mode, use the **class-map type network-qos** command. To remove a class map, use the **no** form of this command.

class-map type network-qos *class_map_name*

no class-map type network-qos *class_map_name*

Syntax Description

class-map-name	Name assigned to the class map. The name class-default is reserved. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Class maps of type network qos support only the **match cos** command.

Examples

This example shows how to create or modify a network qos class map:

```
switch(config)# class-map type network-qos my_class1
switch(config-cmap-nq)#
```

This example shows how to remove a network qos class map:

```
switch(config-cmap-nq)# no class-map my_class1
switch(config)#
```

Related Commands

Command	Description
match cos	Defines a traffic class that matches the class of service (CoS) values.
show class-map type queuing	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

description

To add a description to a class map, policy map, or table map, use the **description** command. To remove the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

text	Description for the class map, policy map, or table map. The description can be a maximum of 200 alphanumeric characters.

Command Default

None

Command Modes

Class map type network qos configuration

Class map type qos configuration

Class map type queuing configuration

Policy map type network qos configuration

Policy map type qos configuration

Policy map type queuing configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to add a description to a qos class map:

```
switch(config)# class-map my_class1
switch(config-cmap-qos)# description This class map filters packets that matches an ACL
switch(config-cmap-qos)#
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.
policy-map	Creates or modifies a policy map.
show class-map	Displays class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

flowcontrol

To enable IEEE 802.3x link-level flow control for the selected interface, use the **flowcontrol** command.

flowcontrol [**receive** {**on** | **off**}] [**transmit** {**on** | **off**}]

Syntax Description

receive	(Optional) Sets flow control in the receive direction.
off	Disables flow control traffic on an interface.
on	Enables flow control traffic on an interface.
transmit	(Optional) Sets flow control in the transmit direction.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable flow control for traffic received on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# flowcontrol receive on
```

Related Commands

Command	Description
priority-flow-control	Sets the PFC mode for the selected interface.
show interface flowcontrol	Displays the detailed listing of the flow control settings on all interfaces.

Send comments to nx5000-docfeedback@cisco.com

match access-group

To identify a specified access control list (ACL) group as a match criteria for a class map, use the **match access-group** command. To remove an ACL match criteria from a class map, use the **no** form of this command.

match access-group name *acl-name*

no match access-group name *acl-name*

Syntax Description

name *acl-name*	Matches on the characteristics in the ACL name specified.

Defaults

None

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Note The **permit** and **deny** ACL keywords do not affect the matching of packets.

Examples

This example shows how to create a qos class map that matches characteristics of the ACL my_acl:

```
switch(config)# class-map class_acl
switch(config-cmap-qos)# match access-group name my_acl
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

match cos

To define the class of traffic using the class of service (CoS) value in a type qos class map, use the **match cos** command. To remove the match on the CoS value, use the **no** form of this command.

match [**not**] **cos** *cos-list*

no match [**not**] **cos** *cos-list*

Syntax Description

not	(Optional) Negates the specified match result.
cos-list	Specified CoS value or list of specified CoS values. Valid values are from 0 to 7.

Defaults

None

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

To specify a list of values, use one of the following options:

- Specify a range of values separated by a dash
- Specify a noncontiguous list of values separated by commas

Note Only class maps of type qos support the optional **not** keyword form of this command. Class maps of type queuing do not support the **not** keyword.

Examples

This example shows how to match on the CoS value for a type qos class map:

```
switch(config)# class-map class_acl
switch(config-cmap-qos)# match cos 5-7
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

match dscp

To identify specific differentiated services code point (DSCP) values as a match criteria, use the **match dscp** command. To remove specified DSCP values as a match criteria, use the **no** form of this command.

match [**not**] **dscp** *dscp-list*

no match [**not**] **dscp** *dscp-list*

Syntax Description

not	(Optional) Negates the specified match result.
dscp-list	Specified DSCP value or list of DSCP values. See Table 5-1 for a list of valid DSCP values.

Defaults

None

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The standard DSCP values are shown in Table 5-1.

To specify a list of values, use one of the following options:

Table 5-1 Standard DSCP Values

	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14
af21	AF21 dscp (010010)—decimal value 18
af22	AF22 dscp (010100)—decimal value 20
af23	AF23 dscp (010110)—decimal value 22
af31	AF31 dscp (011010)—decimal value 26
af32	AF40 dscp (011100)—decimal value 28
af33	AF33 dscp (011110)—decimal value 30
af41	AF41 dscp (100010)—decimal value 34
af42	AF42 dscp (100100)—decimal value 36
af43	AF43 dscp (100110)—decimal value 38
cs1	CS1 (precedence 1) dscp (001000)—decimal value 8

Send comments to nx5000-docfeedback@cisco.com

Table 5-1 Standard DSCP Values (continued)

	List of DSCP Values
cs2	CS2 (precedence 2) dscp (010000)—decimal value 16
cs3	CS3 (precedence 3) dscp (011000)—decimal value 24
cs4	CS4 (precedence 4) dscp (100000)—decimal value 32
cs5	CS5 (precedence 5) dscp (101000)—decimal value 40
cs6	CS6 (precedence 6) dscp (110000)—decimal value 48
cs7	CS7 (precedence 7) dscp (111000)—decimal value 56
default	Default dscp (000000)—decimal value 0
ef	EF dscp (101110)—decimal value 46

- Specify a range of values separated by a dash
- Specify a noncontiguous list of values separated by commas

Examples

This example shows how to match on DSCP value af21:

```
switch(config)# class-map my_test
switch(config-cmap-qos)# match dscp af21
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) port as a match criteria, use the **match ip rtp** command. To remove the RTP port as a match criteria, use the **no** form of this command.

match [**not**] **ip rtp** *port-list*

no match [**not**] **ip rtp** *port-list*

Syntax Description

not	(Optional) Negates the specified match result.
port-list	Specified UDP port or list of UDP ports that are using RTP. Valid values range from 2000 to 65535.

Defaults

None

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

To specify a list of values, use one of the following options:

- Specify a range of values separated by a dash
- Specify a noncontiguous list of values separated by commas

Examples

This example shows how to match on a port using RTP:

```
switch(config)# class-map my_test
switch(config-cmap-qos)# match ip rtp 2300
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

match precedence

To configure a class map to use the precedence value in the type of service (ToS) byte field of the IP header as a match criteria, use the **match precedence** command. To remove the precedence values as a match criteria, use the **no** form of this command.

match [**not**] **precedence** *precedence-list*

no match [**not**] **precedence** *precedence-list*

Syntax Description

not	(Optional) Negates the specified match result.
precedence-list	Specified IP precedence value or list of IP precedence values specified in bytes. Valid values are shown in Table 5-2.

Defaults

None

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

See Table 5-2 for a list of precedence values.

Table 5-2 Precedence Values

Precedence Value	Description
<0-7>	IP precedence value
critical	Critical precedence (5)
flash	Flash precedence (3)
flash-override	Flash override precedence (4)
immediate	Immediate precedence (2)
internet	Internetwork control precedence (6)
network	Network control precedence (7)
priority	Priority precedence (1)
routine	Routine precedence (0)

To specify a list of values, use one of the following options:

- Specify a range of values separated by a dash
- Specify a noncontiguous list of values separated by commas

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to match on an IP precedence value:

```
switch(config)# class-map my_test
switch(config-cmap-qos)# match precedence 7
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

match protocol

To configure a class map to use a specific protocol as a match criterion, use the **match protocol** command. To remove the specified protocol as a match criteria, use the **no** form of this command.

match [**not**] **protocol** *protocol-name*

no match [**not**] **protocol** *protocol-name*

Syntax Description

not	(Optional) Negates the specified match result.
protocol-name	Specified protocol name. Valid values are shown in Table 5-3.

Defaults

None

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The list of valid protocol names is shown in Table 5-3.

Table 5-3 Protocol Names

Argument	Description
arp	Address Resolution Protocol (ARP)
clns_es	CLNS End Systems
clns_is	CLNS Intermediate System
dhcp	Dynamic Host Configuration (DHCP)
ldp	Label Distribution Protocol (LDP)
netbios	NetBIOS Extended User Interface (NetBEUI)

To specify more than one protocol, enter the command more than once with the desired protocol value each time.

Examples

This example shows how to match on a specified protocol:

```
switch(config)# class-map my_test
switch(config-cmap-qos)# match protocol ldp
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

match qos-group

To configure a class map to use a specific QoS group value as a match criterion, use the **match qos-group** command. To remove the specified protocol as a match criteria, use the **no** form of this command.

match [**not**] **qos-group** *qos-group-list*

no match [**not**] **qos-group** *qos-group-list*

Syntax Description

not	(Optional) Negates the specified match result.
qos-group-list	Specified Qos group value or list of QoS group values specified in bytes. Valid values are from 2 to 5.

Command Default

None

Command Modes

Class map type network-qos configuration

Class map type queuing configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The QoS group is an internal label and is not part of the packet payload or any packet header. The QoS group values have no mathematical significance. For example, a QoS group value of 2 is not greater than 1; the values are used only to internally differentiate QoS groups. As such, this value has local significance only.

You match on the QoS group only in egress policies because its value is undefined until you set it in an ingress policy.

To specify a list of values, use one of the following options:

- Specify a range of values separated by a dash
- Specify a noncontiguous list of values separated by commas

Examples

This example shows how to match on a specified QoS group value:

```
switch(config)# class-map type queuing my_test
switch(config-cmap-qos)# match qos-group 6
switch(config-cmap-qos)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
class-map type network-qos	Creates or modifies a network qos class map.
class-map type queuing	Creates or modifies a queuing class map.
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

mtu

To configure the interfaces on a switch to transfer large frames on a port, use the **mtu** command. To remove the configured maximum transmission unit (MTU), use the **no** form of this command.

mtu *mtu-value*

no mtu *mtu-value*

Syntax Description

mtu-value	MTU value for the class of service (CoS). Valid values are 1500 to 9216.

Command Default

Default MTU value is 1500. For FCoE cos 3, the default is 2158.

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.
4.2(1)N1(1)	The MTU range is changed to 1500 to 9216. On a Cisco Nexus 5000 Series that run a Cisco NX-OS release 4.1(3)N2(1) or earlier, the MTU range is from 1538 to 9216.

Usage Guidelines

You can configure an MTU for each virtual link in the system.

Examples

This example shows how to set an MTU value for a class in a type network-qos policy map:

```
switch(config)# class-map type network-qos my_class1
switch(config-cmap-nq)# match qos-group 1
switch(config-cmap-nq)# exit
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)# class type network-qos my_class1
switch(config-pmap-nq-c)# mtu 5000
switch(config-pmap-nq-c)#
```

Related Commands

Command	Description
show class-map	Displays class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

multicast-optimize

To optimize a class to send multiple packets, use the **multicast-optimize** command.

multicast-optimize

no multicast-optimize

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Multicast traffic in a class will be served by all available multicast queues.

Only one class in a policy map can be configured for multicast optimization.

Examples

This example shows how to enable optimized multicast for a traffic class:

```
switch(config)# policy-map type network-qos my_queue
switch(config-pmap-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-pmap-nq-c)# multicast-optimize
switch(config-pmap-nq-c)#
```

This example shows how to remove the multicast optimization from a traffic class:

```
switch(config)# policy-map type network-qos my_queue
switch(config-pmap-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-pmap-nq-c)# no multicast-optimize
switch(config-pmap-nq-c)#
```

Related Commands

Command	Description
show policy-map	Displays the policy maps.

Send comments to nx5000-docfeedback@cisco.com

pause no-drop

To enable Class Based Flow Control (CBFC) pause characteristics on a class referenced in a type network-qos policy map, use the **pause** command. To disable the CBFC pause characteristics on a class, use the **no** form of this command.

pause no-drop [**pfc-cos** *pfc-cos-list*]

no pause no-drop [**pfc-cos** *pfc-cos-list*]

Syntax Description

pfc-cos	(Optional) CoS values to assert priority flow control (PFC) on.
pfc-cos-list	PFC CoS list. The range is from 0 to 7. Use a comma (,) to separate multiple values, or a hyphen (-) to specify a range of values; for example, 0, 2, 3, or 2-5.

Command Default

By default, pause no-drop is on.

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Ethernet interfaces use priority flow control (PFC) to provide lossless service to no-drop system classes. PFC implements pause frames on a per-class basis and uses the IEEE 802.1p CoS value to identify the classes that require lossless service.

You can configure PFC CoS only for traffic classes that match a criteria other than the CoS value (match cos).

Examples

This example shows how to enable pause no-drop on a class referenced in a type network-qos policy map:

```
switch(config)# class-map type network-qos my_class1
switch(config-cmap-nq)# match qos-group 2
switch(config-cmap-nq)# exit
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)# class type network-qos my_class1
switch(config-pmap-nq-c)# pause no-drop
switch(config-pmap-nq-c)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show class-map type network-qos	Displays type network-qos class maps.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

policy-map type network-qos

To create or modify a policy map and enter the policy map type network-qos configuration mode, use the **policy-map type network-qos** command. To remove a policy map, use the **no** form of this command.

policy-map type network-qos *policy-map-name*

no policy-map type network-qos *policy-map-name*

Syntax Description

policy-map-name	Name assigned to a type network-qos policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Use the **service-policy** command to assign policy maps to interfaces.

Examples

This example shows how to create or modify a type network-qos policy map:

```
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)
```

This example shows how to remove a type network-qos policy map:

```
switch(config-pmap-nq)# no policy-map type network-qos my_policy1
switch(config)
```

Related Commands

Command	Description
class type network-qos	References a type network-qos class map in a policy map.
description	Adds a description to a class map or policy map.
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

policy-map (type qos)

To create or modify a policy map and enter the policy map type qos configuration mode, use the **policy-map** command. To remove a QoS policy map, use the **no** form of this command.

policy-map [**type qos**] [**match-first**] *qos-policy-map-name*

no policy-map [**type qos**] [**match-first**] *qos-policy-map-name*

Syntax Description

type qos	(Optional) Specifies the type qos policy map.
match-first	(Optional) Specifies that policies associated with the first class that matches the packet characteristics are executed. This is the default action if this option is not specified. **Note** Because this is the default action, you do not need to enter this variable; it is here to ensure compatibility with other systems.
qos-policy-map-name	Name assigned to a type qos policy map. The name can be a maximum of 40 alphanumeric characters.

Defaults

The software enters the policy map type qos configuration mode if you enter the **policy-map** command without specifying a type.

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Use the **service-policy** command to assign policy maps to interfaces.

Examples

This example shows how to create or modify a type qos policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)#
```

This example shows how to remove a type qos policy map:

```
switch(config-pmap-qos)# no policy-map my_policy1
```

Related Commands

Command	Description
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

policy-map type queuing

To create or modify a policy map and enter the policy map type queuing configuration mode, use the **policy-map type queuing** command. To remove a policy map, use the **no** form of this command.

policy-map type queuing [**match-first**] *queuing-policy-map-name*

no policy-map type queuing [**match-first**] *queuing-policy-map-name*

Syntax Description

match-first	(Optional) Specifies that policies associated with the first class that matches the packet characteristics are executed. This is the default action if this option is not specified. **Note** Because this is the default action, you do not need to enter this variable; it is here to ensure compatibility with other systems.
queuing-policy-map-name	Name assigned to a type queuing policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

Use the **service-policy** command to assign policy maps to interfaces.

Examples

This example shows how to create or modify a queuing policy map:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)#
```

This example shows how to remove a type queuing policy map:

```
switch(config-pmap-que)# no policy-map type queuing my_policy1
switch(config)#
```

Related Commands

Command	Description
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

priority

To assign a priority to a traffic class in a policy map, use the **priority** command. To remove the mapping, use the **no** form of this command.

priority

no priority

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Policy map type queuing class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

When you configure a strict priority queue for a traffic class in a policy map, the priority class receives preference over other class queues. This queue is serviced before all other queues except queue zero (which carries control traffic, not data traffic).

Examples

This example shows how to map the traffic class to a strict priority queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 8q2t-in-q4
switch(config-pmap-c-que)# priority
switch(config-pmap-que)#
```

Related Commands

Command	Description
show policy-map	Displays the policy maps.

Send comments to nx5000-docfeedback@cisco.com

priority-flow-control

To set the priority-flow-control (PFC) mode for the selected interface, use the **priority-flow-control** command.

priority-flow-control mode {**auto** | **on**}

no priority-flow-control mode {**auto** | **on**}

Syntax Description

auto	Negotiates PFC capability.
on	Force-enables PFC.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to force-enable PFC on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# priority-flow-control mode on
switch(config-if)#
```

Related Commands

Command	Description
flowcontrol	Sets link-level flow control for the selected interface.
show interface flowcontrol	Displays the detailed listing of the flow control settings on all interfaces.
show interface priority-flow-control	Displays the priority flow control details for a specified interface.

Send comments to nx5000-docfeedback@cisco.com

queue-limit

To configure tail drop by setting queue limits on both ingress and egress queues, use the **queue-limit** command. To remove a queue limit, use the **no** form of this command.

queue-limit *queue-size* **bytes**

no queue-limit *queue-size* **bytes**

Syntax Description

queue-size	Queue size threshold (in bytes). The range is from 20480 to 204800.

Command Default

None

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

You can use this command to specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map. The system drops packets that exceed the configured queue-size threshold.

You can use this command only for network-qos class maps that do not have “pause” configured.

Examples

This example shows how to assign a queue limit to a policy map network-qos class:

```
switch(config)# policy-map type network-qos my_queue
switch(config-pmap-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-pmap-nq-c)# queue-limit 10 mbytes
switch(config-pmap-nq-c)#
```

This example shows how to remove a queue limit from a policy map queuing class:

```
switch(config)# policy-map type network-qos my_queue
switch(config-pmap-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-pmap-nq-c)# no queue-limit 10 mbytes
switch(config-pmap-nq-c)#
```

Related Commands

Command	Description
pause no-drop	Enables pause characteristics on a class referenced in a type network-qos policy map.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

service-policy

To attach a policy map to an interface or system policy, use the **service-policy** command. To remove a service-policy from an interface or system policy, use the **no** form of this command.

service-policy {**input** | **type** {**qos input** | **queuing** {**input** | **output**}}} *policy-map-name*

no service-policy {**input** | **type** {**qos input** | **queuing** {**input** | **output**}}} *policy-map-name*

Syntax Description

input	Applies this policy map to packets coming into this interface.
type	(Optional) Specifies whether the policy map is of type qos or queuing.
qos	Specifies a policy map of type qos.
queuing	Specifies a policy map of type queuing.
output	Applies this policy map to packets going out of this interface.
policy-map-name	Name of the policy map to attach to this interface. Only one policy map can be attached to the input and one to the output of a given interface for each of the policy type qos and queuing. The policy map name can be a maximum of 40 alphanumeric characters.

Defaults

None

Command Modes

Interface configuration

System QoS configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.
4.2(1)N1(1)	You can attach a policy map to a system policy.

Usage Guidelines

You can attach one ingress and one egress type queuing policy map to an interface of type port, and port channel. Only one policy map can be attached to the input of a given interface for each of the policy type qos and queuing.

Examples

This example shows how to attach a queuing policy map to the ingress packets of a port interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# service-policy type queuing input my_input_q_policy
switch(config-if)#
```

This example shows how to attach qos type policy maps to the incoming packets of an interface:

```
switch# configure terminal
switch(config)# system qos
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config-sys-qos)# service-policy type queueing output my_policy1
switch(config-sys-qos)#
```

Related Commands

Command	Description
show policy-map interface brief	Displays all interfaces and VLANs with attached service policies in a brief format.
system qos	Configures a system policy.

Send comments to nx5000-docfeedback@cisco.com

set cos (policy map type network-qos)

To assign a class of service (CoS) value for a class of traffic in a type network-qos policy map, use the **set** command. To remove the assigned value from the class, use the **no** form of this command.

set cos *cos-value*

no set cos *cos-value*

Syntax Description

cos-value	CoS value to assign for this class of traffic. The range is from 0 to 7.

Command Default

None

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

You can use this command only on type network-qos policies that are attached to egress ports.

Examples

This example shows how to assign a CoS value for a class of traffic in a type network-qos policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)#
```

This example shows how to remove the assignment of CoS for a class of traffic in a type network-qos policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)# no set cos 3
switch(config-pmap-c-qos)#
```

Related Commands

Command	Description
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

set qos-group

To assign the QoS group identifier for a class of traffic in a type qos policy map, use the **set qos-group** command. To remove the assigned value from the class, use the **no** form of this command.

set qos-group *qos-group-value*

no set qos-group *qos-group-value*

Syntax Description

qos-group-value	QoS group value to assign for this class of traffic. The range is from 0 to 126.

Command Default

None

Command Modes

Policy map type qos class configuration

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

You can set the QoS group identifier value only in ingress policies.

Examples

This example shows how to assign a QoS group identifier for a class of traffic in a type qos policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)# set qos-group 100
switch(config-pmap-c-qos)#
```

Related Commands

Command	Description
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

show class-map type network-qos

To display type network-qos class maps, use the **show class-map type network-qos** command.

show class-map type network-qos [*class-map-name*]

Syntax Description

class-map-name	Name of the class map. The name can be a maximum of 40 alphanumeric characters.

Command Default

Displays all type network-qos class maps if no class map name is specified.

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

If you do not specify the type, the command displays all the class maps configured in the system.

Examples

This example shows how to display all type network-qos class maps:

```
switch(config)# show class-map type network-qos


  Type network-qos class-maps
  ===========================

    class-map type network-qos s1
      match qos-group 2

    class-map type network-qos s2
      match qos-group 3

    class-map type network-qos s3
      match qos-group 4

    class-map type network-qos s4
      match qos-group 5

    class-map type network-qos cu1
      match qos-group 2

    class-map type network-qos cu2
      match qos-group 3

    class-map type network-qos cu3
      match qos-group 4

    class-map type network-qos cu4
```

Send comments to nx5000-docfeedback@cisco.com

```
    match qos-group 5

  class-map type network-qos new
    match qos-group 2

  class-map type network-qos class7
    match qos-group 5

  class-map type network-qos class-0
    match qos-group 2

  class-map type network-qos ip-based
    match qos-group 5

  class-map type network-qos class-1-2
    match qos-group 3

  class-map type network-qos class-4-7
    match qos-group 4

  class-map type network-qos cos-based
    match qos-group 2

  class-map type network-qos class-fcoe
    match qos-group 1

  class-map type network-qos class-flood
    match qos-group 2

  class-map type network-qos cos-based-3
    match qos-group 3

  class-map type network-qos cos-based-4
    match qos-group 4

  class-map type network-qos class-default
    match qos-group 0

  class-map type network-qos class-multicast

  class-map type network-qos class-ip-multicast
    match qos-group 5


switch(config)#
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.

Send comments to nx5000-docfeedback@cisco.com

show class-map type qos

To display type qos class maps, use the **show class-map type qos** command.

show class-map type qos [*class-map-name*]

Syntax Description

class-map-name	Named class map. The name *class-default* is reserved. The name can be a maximum of 40 alphanumeric characters.

Defaults

Displays all type qos class maps if no class map name is specified.

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display all type qos class maps:

```
switch(config)# show class-map type qos


  Type qos class-maps
  ===================

    class-map type qos s1
      match cos 0

    class-map type qos s2
      match protocol ldp
      match ip rtp 2000
      match protocol dhcp
      match protocol arp

    class-map type qos s3
      match access-group name mac

    class-map type qos s4
      match access-group name ipv4

    class-map type qos cp1
      match precedence 4-5
      match cos 0,4
      match dscp 4
      match protocol ldp
      match protocol arp

    class-map type qos cp2
      match ip rtp 2000
      match cos 0
```

Send comments to nx5000-docfeedback@cisco.com

```
class-map type qos cp3
  match access-group name mac

class-map type qos cp5

class-map type qos cq1
  match protocol ldp
  match precedence 7
  match cos 0

class-map type qos cq2
  match protocol ldp
  match cos 1-2

class-map type qos cq3
  match access-group name mac

class-map type qos cq4
  match access-group name ipv4-1

class-map type qos cq5
  match access-group name ipv6-based

class-map type qos p1.1
  match cos 7

class-map type qos p1.2
  match protocol ldp
  match ip rtp 2000-6001,10000-20000,60000-65535
  match dscp 1
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p1.3
  match access-group name mac

class-map type qos p1.4
  match access-group name ipv4

class-map type qos p2.1
  match cos 0,7

class-map type qos p2.2
  match protocol ldp
  match ip rtp 2000-6000,6002,10000-20000,60000-65535
  match dscp 2
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p2.3
  match access-group name mac

class-map type qos p2.4
  match access-group name ipv4

class-map type qos p3.1
  match cos 0,7

class-map type qos p3.2
  match protocol ldp
  match ip rtp 2000-6000,6003,10000-20000,60000-65535
  match dscp 3
```

Send comments to nx5000-docfeedback@cisco.com

```
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p3.3
  match access-group name mac

class-map type qos p3.4
  match access-group name ipv4

class-map type qos p4.1
  match cos 0,7

class-map type qos p4.2
  match protocol ldp
  match ip rtp 2000-6000,6004,10000-20000,60000-65535
  match dscp 4
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p4.3
  match access-group name mac

class-map type qos p4.4
  match access-group name ipv4

class-map type qos p5.1
  match cos 0,7

class-map type qos p5.2
  match protocol ldp
  match ip rtp 2000-6000,6005,10000-20000,60000-65535
  match dscp 5
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p5.3
  match access-group name mac

class-map type qos p5.4
  match access-group name ipv4

class-map type qos p6.1
  match cos 0,7

class-map type qos p6.2
  match protocol ldp
  match ip rtp 2000-6000,6006,10000-20000,60000-65535
  match dscp 6
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p6.3
  match access-group name mac

class-map type qos p6.4
  match access-group name ipv4

class-map type qos p7.1
  match cos 0,7
```

Send comments to nx5000-docfeedback@cisco.com

```
class-map type qos p7.2
  match protocol ldp
  match ip rtp 2000-6000,6007,10000-20000,60000-65535
  match dscp 7
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p7.3
  match access-group name mac

class-map type qos p7.4
  match access-group name ipv4

class-map type qos p8.1
  match cos 0,7

class-map type qos p8.2
  match protocol ldp
  match ip rtp 2000-6000,6008,10000-20000,60000-65535
  match dscp 8
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p8.3
  match access-group name mac

class-map type qos p8.4
  match access-group name ipv4

class-map type qos p9.1
  match cos 0,7

class-map type qos p9.2
  match protocol ldp
  match ip rtp 2000-6000,6009,10000-20000,60000-65535
  match dscp 9
  match protocol dhcp
  match protocol arp
  match precedence 0-7

class-map type qos p9.3
  match access-group name mac

class-map type qos p9.4
  match access-group name ipv4

class-map type qos class-0
  match cos 0

class-map type qos class-6
  match cos 6

class-map type qos class-7
  match cos 7

class-map type qos clsas-0

class-map type qos cos-6-7
  match cos 7

class-map type qos ip-based
  match access-group name ip-based
```

Send comments to nx5000-docfeedback@cisco.com

```
    class-map type qos acl-based
      match access-group name ipPacl

    class-map type qos class-1-2
      match cos 1-2

    class-map type qos class-4-5
      match cos 4-5

    class-map type qos class-4-6
      match cos 5

    class-map type qos class-4-7
      match cos 5,7

    class-map type qos class-405

    class-map type qos cos-based

    class-map type qos mac-based
      match access-group name foo

    class-map type qos udp-based
      match access-group name ip-based

    class-map type qos class-fcoe
      match cos 3

    class-map type qos class-flood

    class-map type qos class-default
      match any

    class-map type qos class-all-flood
      match all flood

    class-map type qos class-ip-multicast
      match ip multicast

switch(config)#
```

This example shows how to display a specific class map:

```
switch# show class-map type qos class-4-6


  Type qos class-maps
  ===================

    class-map type qos class-4-6
      match cos 5

switch#
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.

Send comments to nx5000-docfeedback@cisco.com

show class-map type queuing

To display type queuing class maps, use the **show class-map type queuing** command.

show class-map type queuing [*class-map-name*]

Syntax Description

class-map-name	Named class map. The name can be a maximum of 40 alphanumeric characters.

Defaults

Displays all type queuing class maps if no class map name is specified.

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display all type queuing class maps:

```
switch(config)# show class-map type queuing


  Type queuing class-maps
  ========================

    class-map type queuing s1
      match qos-group 2

    class-map type queuing s2
      match qos-group 3

    class-map type queuing s3
      match qos-group 4

    class-map type queuing s4
      match qos-group 5

    class-map type queuing cq1
      match qos-group 2

    class-map type queuing cq2
      match qos-group 3

    class-map type queuing cq3
      match qos-group 4

    class-map type queuing cq4
      match qos-group 5

    class-map type queuing pq1
```

Send comments to nx5000-docfeedback@cisco.com

```
    class-map type queuing cqe1
      match qos-group 2

    class-map type queuing cqe2
      match qos-group 3

    class-map type queuing cqe3
      match qos-group 4

    class-map type queuing cqe4
      match qos-group 5

    class-map type queuing p1.1
      match qos-group 2

    class-map type queuing p1.2
      match qos-group 3

    class-map type queuing p1.3
      match qos-group 4

    class-map type queuing p1.4
      match qos-group 5

    class-map type queuing p2.1
      match qos-group 2

    class-map type queuing p2.2
      match qos-group 3

    class-map type queuing p2.3
      match qos-group 4

    class-map type queuing p2.4
      match qos-group 5

    class-map type queuing p3.1
      match qos-group 2

    class-map type queuing p3.2
      match qos-group 3

--More--
switch(config)#
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.

Send comments to nx5000-docfeedback@cisco.com

show interface flowcontrol

To display the detailed listing of the flow control settings on all interfaces, use the **show interface flowcontrol** command.

show interface flowcontrol [**module** *number*]

Syntax Description

module *number*	(Optional) Displays flow control settings on all interfaces on a specified module. The module *number* range is from 1 to 3.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the flow control settings on all interfaces on a switch:

```
switch# show interface flowcontrol

--------------------------------------------------------------------------------
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
--------------------------------------------------------------------------------
Eth1/1       off      off      off      off         0                 0

Eth1/2       off      off      off      off         0                 0

Eth1/3       off      off      off      off         0                 0

Eth1/4       off      off      off      off         0                 0

Eth1/5       off      off      off      off         0                 0

Eth1/6       off      off      off      off         0                 0

Eth1/7       off      off      off      off         0                 0

Eth1/8       off      off      off      off         0                 0

Eth1/9       off      off      off      off         0                 0

Eth1/10      off      off      off      off         0                 0

Eth1/11      off      off      off      off         0                 0

--More--
switch#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the flow control settings on all interfaces on a specified module:

```
switch# show interface flowcontrol module 1

--------------------------------------------------------------------------------
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
--------------------------------------------------------------------------------
Eth1/1       off      off      off      off         0                 0

Eth1/2       off      off      off      off         0                 0

Eth1/3       off      off      off      off         0                 0

Eth1/4       off      off      off      off         0                 0

Eth1/5       off      off      off      off         0                 0

Eth1/6       off      off      off      off         0                 0

Eth1/7       off      off      off      off         0                 0

Eth1/8       off      off      off      off         0                 0

Eth1/9       off      off      off      off         0                 0

Eth1/10      off      off      off      off         0                 0

Eth1/11      off      off      off      off         0                 0

Eth1/12      off      off      off      off         0                 0

Eth1/13      off      off      off      off         0                 0

Eth1/14      off      off      off      off         0                 0
--More--
switch#
```

Related Commands

Command	Description
flowcontrol	Enables IEEE 802.3x link-level flow control on interfaces.
priority-flow-control	Sets the priority-flow-control (PFC) mode for the selected interface.

Send comments to nx5000-docfeedback@cisco.com

show interface priority-flow-control

To display the priority flow control details for a specified interface, use the **show interface priority-flow-control** command.

show interface [**ethernet** *slot/port*] **priority-flow-control**

Syntax Description

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

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the priority flow control details for a specified interface:

```
switch# show interface ethernet 1/2 priority-flow-control
============================================================
Port               Mode Oper(VL bmap)  RxPPP      TxPPP
============================================================

Ethernet1/2        Auto On  (9)       4088353    1890
switch#
```

The interface specified is Ethernet 1/2, the PFC mode is set to negotiate PFC capability, the operation is on, and packets transmitted is 1890.

Related Commands

Command	Description
priority-flow-control	Sets the PFC mode for the selected interface.

Send comments to nx5000-docfeedback@cisco.com

show interface untagged-cos

To display the untagged class of service (CoS) values for a specified interface, use the **show interface untagged-cos** command.

show interface untagged-cos [**module** *module_no*]

Syntax Description

module	(Optional) Displays the interfaces on this module of the switch chassis.
module_no	Module number in switch chassis. The range is from 1 to 18.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the untagged CoS values for a specified interface:

```
switch# show interface untagged-cos
================================

Interface      Untagged-CoS
================================

port-channel1
port-channel3  2
port-channel5  5
port-channel6
port-channel12
port-channel15
port-channel20
port-channel24
port-channel25
port-channel33
port-channel41
port-channel44
--More--
switch#
```

Related Commands

Command	Description
untagged cos	Sets a CoS value for untagged Ethernet frames.

Send comments to nx5000-docfeedback@cisco.com

show policy-map

To display policy maps, use the **show policy-map** command.

show policy-map [**type** {**qos** | **queuing** | **network-qos**}] [*policy-map-name*]

Syntax Description

type	(Optional) Specifies the component type to display.
network-qos	Displays policy maps of type network-qos.
qos	Displays policy maps of type qos only.
queuing	Displays policy maps of type queuing only.
policy-map-name	(Optional) Named policy map. The name can be a maximum of 40 alphanumeric characters.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

When you enter the **show policy-map** command with no arguments or keywords, the system also displays the Control Plane Policing (CoPP) information.

Examples

This example shows how to display a named network-qos policy map:

```
switch# show policy-map type network-qos my_pnq


  Type network-qos policy-maps
  ============================

  policy-map type network-qos my_pnq
    class type network-qos cl_nq
      multicast-optimize
      queue-limit 20480 bytes
      mtu 1500
    class type network-qos class-fcoe
      pause no-drop
      mtu 2158
    class type network-qos class-default
      mtu 1500
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
policy-map	Creates or modifies a policy map.
show queuing interface	Displays QoS statistics.

Send comments to nx5000-docfeedback@cisco.com

show policy-map interface

To display service policy maps configured on the interfaces, use the **show policy-map interface** command.

show policy-map interface [**ethernet** {*slot/port*} | **port-channel** {*channel-number***}**] [**input** | **output**] [**type** {**qos** | **queuing**}]

Syntax Description

ethernet	(Optional) Displays policy maps assigned to Ethernet interfaces.
slot/port	Ethernet interface slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel	(Optional) Displays policy maps assigned to EtherChannels.
channel-number	EtherChannel number. The number is from 1 to 4096.
input	(Optional) Displays policy maps assigned to input traffic only.
output	(Optional) Displays policy maps assigned to output traffic only.
type	(Optional) Specifies the component type to display.
qos	Displays policy maps of type qos only.
queuing	Displays policy maps of type queuing only.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Statistics are on by default.

Examples

This example shows how to display policy maps assigned to a specified interface:

```
switch(config)# show policy-map interface ethernet 2/10
```

This example shows how to display QoS policy maps assigned to a specified interface:

```
switch# show policy-map interface ethernet 3/1 type qos


Global statistics status :   disabled

Ethernet3/1

  Service-policy (qos) input:   s
    policy statistics status:   disabled
```

Send comments to nx5000-docfeedback@cisco.com

```
    Class-map (qos):   s1 (match-any)
      Match: cos 0
      set qos-group 2

    Class-map (qos):   class-1-2 (match-any)
      Match: cos 1-2
      set qos-group 3

    Class-map (qos):   class-4-5 (match-any)
      Match: cos 4-5
      set qos-group 4

    Class-map (qos):   class-6 (match-any)
      Match: cos 6
      set qos-group 5

    Class-map (qos):   class-fcoe (match-any)
      Match: cos 3
      set qos-group 1

    Class-map (qos):   class-default (match-any)
      Match: any
      set qos-group 0

switch#
```

This example shows how to display the policy maps assigned to the output traffic of a specified interface:

```
switch# show policy-map interface ethernet 3/1 output


Global statistics status :   disabled

Ethernet3/1

  Service-policy (queuing) output:   pqe1
    policy statistics status:   disabled

    Class-map (queuing):   cqe1 (match-any)
      Match: qos-group 2
      bandwidth percent 20

    Class-map (queuing):   cqe2 (match-any)
      Match: qos-group 3
      priority

    Class-map (queuing):   cqe3 (match-any)
      Match: qos-group 4
      bandwidth percent 20

    Class-map (queuing):   cqe4 (match-any)
      Match: qos-group 5
      bandwidth percent 40

    Class-map (queuing):   class-fcoe (match-any)
      Match: qos-group 1
      bandwidth percent 10

    Class-map (queuing):   class-default (match-any)
      Match: qos-group 0
      bandwidth percent 5

switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
policy-map	Creates or modifies a policy map.
show queuing interface	Displays QoS statistics.

Send comments to nx5000-docfeedback@cisco.com

show policy-map interface brief

To display policy maps applied to interfaces in a brief format, use the **show policy-map interface brief** command.

show policy-map interface brief

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display assigned policy maps in a brief format:

```
switch(config)# show policy-map interface brief


 Interface      [Status]:INP QOS        INP QUE       OUT QUE
====================================================================
port-channel1   [Active]:p1            pqe1          pqe1
port-channel3   [Active]:s             pqe1          pqe1
port-channel5   [Active]:s             pqe1          pqe1
port-channel6   [Active]:s             pqe1          pqe1
port-channel12  [Active]:p12           p12-in        p12-out
port-channel15  [Active]:s             pqe1          pqe1
port-channel20  [Active]:s             pqe1          pqe1
port-channel24  [Active]:p4            pqe1          pqe1
port-channel25  [Active]:p4            pqe1          pqe1
port-channel33  [Active]:s             pqe1          pqe1
port-channel41  [Active]:s             pqe1          pqe1
port-channel44  [Active]:s             pqe1          pqe1
port-channel48  [Active]:s             pqe1          pqe1
port-channel101 [Active]:s             pqe1          pqe1
port-channel102 [Active]:p4
port-channel103 [Active]:p4
port-channel104 [Active]:p4
port-channel105 [Active]:p4
port-channel106 [Active]:p4
port-channel107 [Active]:p4
--More--
switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
policy-map	Creates or modifies a policy map.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

show policy-map system

To display all active policy maps in the system, use the **show policy-map** system command.

show policy-map system [**type** {**network-qos** | **qos** [**input**] | **queuing** [**input** | **output**]}]

Syntax Description

type	(Optional) Specifies the component type to display.
network-qos	Displays policy maps of type network-qos only.
qos	Displays policy maps of type qos only.
input	(Optional) Displays policy maps assigned to input traffic.
queuing	Displays policy maps of type queuing only.
output	(Optional) Displays policy maps assigned to output traffic.

Command Default

All policy maps

Command Modes

EXEC mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

If you do not specify a policy map type and name, the system displays all the active policy maps in the system.

Examples

This example shows how to display all active policy maps in the system:

```
switch# show policy-map system


  Type network-qos policy-maps
  ============================

  policy-map type network-qos s
    class type network-qos s2      match qos-group 3

      mtu 4000
    class type network-qos s1      match qos-group 2

      mtu 5000
      set cos 0
      multicast-optimize
      pause no-drop
    class type network-qos s3      match qos-group 4

      mtu 9216
    class type network-qos s4      match qos-group 5
```

Send comments to nx5000-docfeedback@cisco.com

```
    mtu 9216
  class type network-qos class-fcoe      match qos-group 1

    pause no-drop
    mtu 2158
  class type network-qos class-default      match qos-group 0

    mtu 1500


Service-policy (qos) input:   s
  policy statistics status:   disabled

  Class-map (qos):   s1 (match-any)
    Match: cos 0
    set qos-group 2

  Class-map (qos):   class-1-2 (match-any)
    Match: cos 1-2
    set qos-group 3

  Class-map (qos):   class-4-5 (match-any)
    Match: cos 4-5
    set qos-group 4

  Class-map (qos):   class-6 (match-any)
    Match: cos 6
    set qos-group 5

  Class-map (qos):   class-fcoe (match-any)
    Match: cos 3
    set qos-group 1

  Class-map (qos):   class-default (match-any)
    Match: any
    set qos-group 0

Service-policy (queuing) input:   pqe1
  policy statistics status:   disabled

  Class-map (queuing):   cqe1 (match-any)
    Match: qos-group 2
    bandwidth percent 20

  Class-map (queuing):   cqe2 (match-any)
    Match: qos-group 3
    priority

  Class-map (queuing):   cqe3 (match-any)
    Match: qos-group 4
    bandwidth percent 20

  Class-map (queuing):   cqe4 (match-any)
    Match: qos-group 5
    bandwidth percent 40

  Class-map (queuing):   class-fcoe (match-any)
    Match: qos-group 1
    bandwidth percent 10

  Class-map (queuing):   class-default (match-any)
    Match: qos-group 0
    bandwidth percent 5
```

Send comments to nx5000-docfeedback@cisco.com

```
  Service-policy (queuing) output:   pqe1
    policy statistics status:   disabled

    Class-map (queuing):   cqe1 (match-any)
      Match: qos-group 2
      bandwidth percent 20

    Class-map (queuing):   cqe2 (match-any)
      Match: qos-group 3
      priority

    Class-map (queuing):   cqe3 (match-any)
      Match: qos-group 4
      bandwidth percent 20

    Class-map (queuing):   cqe4 (match-any)
      Match: qos-group 5
      bandwidth percent 40

    Class-map (queuing):   class-fcoe (match-any)
      Match: qos-group 1
      bandwidth percent 10

    Class-map (queuing):   class-default (match-any)
      Match: qos-group 0
      bandwidth percent 5

switch#
```

This example shows how to display active network-qos policy maps in the system:

```
switch# show policy-map system type network-qos


  Type network-qos policy-maps
  ============================

  policy-map type network-qos s
    class type network-qos s2      match qos-group 3

      mtu 4000
    class type network-qos s1      match qos-group 2

      mtu 5000
      set cos 0
      multicast-optimize
      pause no-drop
    class type network-qos s3      match qos-group 4

      mtu 9216
    class type network-qos s4      match qos-group 5

      mtu 9216
    class type network-qos class-fcoe      match qos-group 1

      pause no-drop
      mtu 2158
    class type network-qos class-default      match qos-group 0

      mtu 1500
switch#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show policy-map	Displays all policy maps.

Send comments to nx5000-docfeedback@cisco.com

show queuing interface

To display the queuing information on interfaces, use the **show queuing interface** command.

show queuing interface [**ethernet** *slot-no*/*port-no*]

Syntax Description

ethernet	(Optional) Specifies that queuing information to be displayed for an Ethernet interface.
slot-no	Slot number of the Ethernet interface. The range is from 1 to 255.
port-no	Port number of the Ethernet interface. The range is from 1 to 128.

Command Default

Displays the queuing information for all interfaces.

Command Modes

EXEC mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the queuing information for all interfaces:

```
switch# show queuing interface
Ethernet1/1 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR             73
        1       WRR              0
        2       WRR              1
        3       WRR              6
        4       WRR             20
        5       priority         0

  RX Queuing
    qos-group 0
    q-size: 25600, HW MTU: 9280 (9216 configured)
    drop-type: drop, xon: 0, xoff: 160
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 1
    q-size: 76800, HW MTU: 2240 (2158 configured)
    drop-type: no-drop, xon: 128, xoff: 240
    Statistics:
        Pkts received over the port             : 0
```

Send comments to nx5000-docfeedback@cisco.com

```
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 2
    q-size: 20480, HW MTU: 9280 (9216 configured)
    drop-type: drop, xon: 0, xoff: 128
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 3
    q-size: 20480, HW MTU: 9280 (9216 configured)
    drop-type: drop, xon: 0, xoff: 128
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 4
    q-size: 20480, HW MTU: 9280 (9216 configured)
    drop-type: drop, xon: 0, xoff: 128
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 5
    q-size: 81920, HW MTU: 9280 (9216 configured)
    drop-type: no-drop, xon: 128, xoff: 230
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

  Total Multicast crossbar statistics:
    Mcast pkts received from the cross-bar      : 0

Ethernet1/2 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR             73
        1       WRR              0
        2       WRR              1
```

Send comments to nx5000-docfeedback@cisco.com

```
        3       WRR              6
        4       WRR             20
        5       priority         0
<---output truncated--->
switch#
```

This example shows how to display the queuing information on Ethernet interface 1/2:

```
switch# show queuing interface ethernet 1/2
Ethernet1/2 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR             73
        1       WRR              0
        2       WRR              1
        3       WRR              6
        4       WRR             20
        5       priority         0

  RX Queuing
    qos-group 0
    q-size: 25600, HW MTU: 9280 (9216 configured)
    drop-type: drop, xon: 0, xoff: 160
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 1851526994
        Pkts sent to the port                   : 1851527000
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 1
    q-size: 76800, HW MTU: 2240 (2158 configured)
    drop-type: no-drop, xon: 128, xoff: 240
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

    qos-group 2
    q-size: 20480, HW MTU: 9280 (9216 configured)
    drop-type: drop, xon: 0, xoff: 128
    Statistics:
        Pkts received over the port             : 0
        Ucast pkts sent to the cross-bar        : 0
        Mcast pkts sent to the cross-bar        : 0
        Ucast pkts received from the cross-bar  : 0
        Pkts sent to the port                   : 0
        Pkts discarded on ingress               : 0
        Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

--More--
switch#
```

Table 5-4 describes the significant fields shown in the display.

Send comments to nx5000-docfeedback@cisco.com

Table 5-4 show queuing interface Field Descriptions

Field	Description
Ethernet ...	Ethernet interface information.
qoS-group	Information about QoS groups configured on the switch.
sched-type	Type of schedule.
WRR	Weighted round robin(WRR). Queue eight for scheduling.
Priority	Priority of the queue.
q-size	Queue size.
drop-type	Queue drop type can be either drop or no-drop.
MTU	Maximum transmit unit (MTU) for the queue.
Xon	Transmission on at this threshold.
Xoff	Transmission off at this threshold.

Related Commands

Command	Description
hardware buffer-threshold	Configures the hardware buffer threshold.
hardware queue-limit	Configures the hardware queue limit.
show fex	Displays all configured Fabric Extender chassis connected to the switch.

Send comments to nx5000-docfeedback@cisco.com

system jumbomtu

To define the upper bound of any maximum transmission unit (MTU) in the system, use the **system jumbomtu** command.

system jumbomtu [**value**]

Syntax Description

value	Jumbomtu value. The range is from 2158 to 9216.

Command Default

9216 bytes

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to define the upper bound of any MTU in the system:

```
switch(config)# system jumbomtu 9216
switch(config)#
```

Related Commands

Command	Description
show interface	Displays the jumbo MTU frames sent and received on the specified interface.

Send comments to nx5000-docfeedback@cisco.com

system qos

To configure a system policy, use the **system qos** command.

system qos

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure a system qos to apply a queuing policy to all interfaces in the system:

```
switch(config)# system qos
switch(config-sys-qos)#
```

Related Commands

Command	Description
service-policy	Associates the system class policy-map to the service policy for the system.

Send comments to nx5000-docfeedback@cisco.com

untagged cos

To override the class of service (CoS) value for the selected interface, use the **untagged cos** command. To revert to the defaults, use the **no** form of this command.

untagged cos *cos-value*

no untagged cos *cos-value*

Syntax Description

cos-value	Class of service (CoS) value for untagged frames. Values can range from 1 to 7.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

Ethernet frames received with no CoS value are given a CoS value of 0.

Examples

This example shows how to set the CoS value to 4 for untagged frames received on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# untagged cos 4
```

Related Commands

Command	Description
match cos	Sets the CoS value to match for the selected class.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 6

Security Commands

This chapter describes the Cisco NX-OS security commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

aaa accounting default

To configure authentication, authorization, and accounting (AAA) methods for accounting, use the **aaa accounting default** command. To revert to the default, use the **no** form of this command.

aaa accounting default {**group** {*group-list*} | **local**}

no aaa accounting default {**group** {*group-list*} | **local**}

Syntax Description

group	Specifies that a server group be used for accounting.
group-list	Space-delimited list that specifies one or more configured RADIUS server groups.
local	Specifies that the local database be used for accounting.

Command Default

The local database is the default.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **group** *group-list* method refers to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method, or **local** method and they fail, then the accounting authentication can fail.

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch(config)# aaa accounting default group
```

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
radius-server host	Configures RADIUS servers.
show aaa accounting	Displays AAA accounting status information.
tacacs-server host	Configures TACACS+ servers.

Send comments to nx5000-docfeedback@cisco.com

aaa authentication login console

To configure authentication, authorization, and accounting (AAA) authentication methods for console logins, use the **aaa authentication login console** command. To revert to the default, use the **no** form of this command.

aaa authentication login console {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

Syntax Description

group	Specifies to use a server group for authentication.
group-list	Space-separated list of RADIUS or TACACS+ server groups. The list can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • Any configured RADIUS or TACACS+ server group name.
none	(Optional) Specifies to use the username for authentication.
local	(Optional) Specifies to use the local database for authentication.

Command Default

The local database

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method or **local** method and they fail, then the authentication can fail. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

Examples

This example shows how to configure the AAA authentication console login method:

```
switch(config)# aaa authentication login console group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
switch(config)# no aaa authentication login console group radius
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
tacacs-server host	Configures TACACS+ servers.

Send comments to nx5000-docfeedback@cisco.com

aaa authentication login default

To configure the default authentication, authorization, and accounting (AAA) authentication methods, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

Syntax Description

group	Specifies that a server group be used for authentication.
group-list	Space-separated list of RADIUS or TACACS+ server groups that can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • Any configured RADIUS or TACACS+ server group name.
none	(Optional) Specifies that the username be used for authentication.
local	(Optional) Specifies that the local database be used for authentication.

Command Default

The local database

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method or **local** method and they fail, then the authentication fails. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

Examples

This example shows how to configure the AAA authentication console login method:

```
switch(config)# aaa authentication login default group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
switch(config)# no aaa authentication login default group radius
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
tacacs-server host	Configures TACACS+ servers.

Send comments to nx5000-docfeedback@cisco.com

aaa authentication login error-enable

To configure that the authentication, authorization, and accounting (AAA) authentication failure message displays on the console, use the **aaa authentication login error-enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login error-enable

no aaa authentication login error-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When you log in, the login is processed by rolling over to the local user database if the remote AAA servers do not respond. In this situation, the following message is displayed if you have enabled the displaying of login failure messages:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

Examples

This example shows how to enable the display of AAA authentication failure messages to the console:

```
switch(config)# aaa authentication login error-enable
```

This example shows how to disable the display of AAA authentication failure messages to the console:

```
switch(config)# no aaa authentication login error-enable
```

Related Commands

Command	Description
show aaa authentication	Displays the status of the AAA authentication failure message display.

Send comments to nx5000-docfeedback@cisco.com

aaa authentication login mschap enable

To enable Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication at login, use the **aaa authentication login mschap enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschap enable

no aaa authentication login mschap enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable MS-CHAP authentication:

```
switch(config)# aaa authentication login mschap enable
```

This example shows how to disable MS-CHAP authentication:

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the status of MS-CHAP authentication.

Send comments to nx5000-docfeedback@cisco.com

aaa authorization commands default

To configure default authentication, authorization, and accounting (AAA) authorization methods for all EXEC commands, use the **aaa authorization commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization commands default [**group** *group-list*] [**local** | **none**]

no aaa authorization commands default [**group** *group-list*] [**local** | **none**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	List of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name. The name can be a space-separated list of server groups, and a maximum of 127 characters.
local	(Optional) Specifies to use the local role-based database for authorization.
none	(Optional) Specifies to use no database for authorization.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature by using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The local method or the none method is used only if all the configured server groups fail to respond and you have configured **local** or **none** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you specify the **none** method alone or after the **group** method, then the authorization always succeeds.

Examples

This example shows how to configure the default AAA authorization methods for EXEC commands:

Send comments to nx5000-docfeedback@cisco.com

```
switch(config)# aaa authorization commands default group TacGroup local
switch(config)#
```

This example shows how to revert to the default AAA authorization methods for EXEC commands:

```
switch(config)# no aaa authorization commands default group TacGroup local
switch(config)#
```

Related Commands

Command	Description
aaa authorization config-commands default	Configures default AAA authorization methods for configuration commands.
aaa server group	Configures AAA server groups.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
tacacs-server host	Configures a TACACS+ server.

Send comments to nx5000-docfeedback@cisco.com

aaa authorization config-commands default

To configure the default authentication, authorization, and accounting (AAA) authorization methods for all configuration commands, use the **aaa authorization config-commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization config-commands default [**group** *group-list*] [**local** | **none**]

no aaa authorization config-commands default [**group** *group-list*] [**local** | **none**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	List of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name. The name can be a space-separated list of server groups, and a maximum of 127 characters.
local	(Optional) Specifies to use the local role-based database for authorization.
none	(Optional) Specifies to use no database for authorization.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature by using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The local method or the none method is used only if all the configured server groups fail to respond and you have configured **local** or **none** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you specify the **none** method alone or after the **group** method, then the authorization always succeeds.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to configure the default AAA authorization methods for configuration commands:

```
switch(config)# aaa authorization config-commands default group TacGroup local
switch(config)#
```

This example shows how to revert to the default AAA authorization methods for configuration commands:

```
switch(config)# no aaa authorization config-commands default group TacGroup local
switch(config)#
```

Related Commands

Command	Description
aaa authorization commands default	Configures default AAA authorization methods for EXEC commands.
aaa server group	Configures AAA server groups.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
tacacs-server host	Configures a TACACS+ server.

Send comments to nx5000-docfeedback@cisco.com

aaa group server radius

To create a RADIUS server group and enter RADIUS server group configuration mode, use the **aaa group server radius** command. To delete a RADIUS server group, use the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	RADIUS server group name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to create a RADIUS server group and enter RADIUS server configuration mode:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
switch(config)# no aaa group server radius RadServer
```

Related Commands

Command	Description
show aaa groups	Displays server group information.

Send comments to nx5000-docfeedback@cisco.com

aaa user default-role

To enable the default role assigned by the authentication, authorization, and accounting (AAA) server administrator for remote authentication, use the **aaa user default-role** command. To disable the default role, use the **no** form of this command.

aaa user default-role

no aaa user default-role

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable the default role assigned by the AAA server administrator for remote authentication:

```
switch# aaa user default-role
switch#
```

This example shows how to disable the default role assigned by the AAA server administrator for remote authentication:

```
switch# no aaa user default-role
switch#
```

Related Commands

Command	Description
show aaa user default-role	Displays the status of the default user for remote authentication.
show aaa authentication	Displays AAA authentication information.

Send comments to nx5000-docfeedback@cisco.com

action

To specify what the switch does when a packet matches a **permit** command in a VLAN access control list (VACL), use the **action** command. To remove an **action** command, use the **no** form of this command.

action {**drop forward**}

no action {**drop forward**}

Syntax Description

drop	Specifies that the switch drops the packet.
forward	Specifies that the switch forwards the packet to its destination port.

Command Default

None

Command Modes

VLAN access-map configuration

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **action** command specifies the action that the device takes when a packet matches the conditions in the ACL specified by the **match** command.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

Related Commands

Command	Description
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
statistics	Enables statistics for an access control list or VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send comments to nx5000-docfeedback@cisco.com

clear access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv4 ACL whose counters the switch clears. The name can be a maximum of 64 alphanumeric characters.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear counters for all IPv4 ACLs:

```
switch# clear access-list counters
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
```

Related Commands

Command	Description
access-class	Applies an IPv4 ACL to a VTY line.
ip access-group	Applies an IPv4 ACL to an interface.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.

Send comments to nx5000-docfeedback@cisco.com

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the accounting log:

```
switch# clear accounting log
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

Send comments to nx5000-docfeedback@cisco.com

clear ip arp

To clear the Address Resolution Protocol (ARP) table and statistics, use the **clear ip arp** command.

clear ip arp [**vlan** *vlan-id* [**force-delete** | **vrf** {*vrf-name* | **all** | **default** | **management**}]]

Syntax Description

vlan *vlan-id*	(Optional) Clears the ARP information for a specified VLAN. The range is from 1 to 4094, except for the VLANs reserved for internal use.
force-delete	(Optional) Clears the entries from ARP table without refresh.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) to clear from the ARP table.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the ARP table.
default	Specifies that the default VRF entry be cleared from the ARP table.
management	Specifies that the management VRF entry be cleared from the ARP table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to clear the ARP table statistics:

```
switch# clear ip arp
switch#
```

This example shows how to clear the ARP table statistics for VLAN 10 with the VRF vlan-vrf:

```
switch# clear ip arp vlan 10 vrf vlan-vrf
switch#
```

Related Commands

Command	Description
show ip arp	Displays the ARP configuration status.

Send comments to nx5000-docfeedback@cisco.com

deadtime

To configure the dead-time interval for a RADIUS or TACACS+ server group, use the **deadtime** command. To revert to the default, use the **no** form of this command.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Number of minutes for the interval. The range is from 0 to 1440 minutes. Setting the dead-time interval to 0 disables the timer.

Command Default

0 minutes

Command Modes

RADlUS server group configuration

TACACS+ server group configuration

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS.

Examples

This example shows how to set the dead-time interval to 2 minutes for a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

This example shows how to revert to the dead-time interval default:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

Send comments to nx5000-docfeedback@cisco.com

deny (IPv4)

To create an IPv4 access control list (ACL) rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no deny *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Send comments to nx5000-docfeedback@cisco.com

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following: – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

Send comments to nx5000-docfeedback@cisco.com

dscp *dscp*	(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **ef**—Expedited Forwarding (101110)

Send comments to nx5000-docfeedback@cisco.com

precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical**—Precedence 5 (101) • **flash**—Precedence 3 (011) • **flash-override**—Precedence 4 (100) • **immediate**—Precedence 2 (010) • **internet**—Precedence 6 (110) • **network**—Precedence 7 (111) • **priority**—Precedence 1 (001) • **routine**—Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(Optional; IGMP only) Rule that matches only packets of the specified ICMP message type. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.
igmp-message	(Optional; IGMP only) Rule that matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace

Send comments to nx5000-docfeedback@cisco.com

operator port [*port*]	(Optional; TCP and UDP only) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than the *port* argument. • **lt**—Matches only if the port in the packet is less than the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
flags	(Optional; TCP only) Rule that matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(Optional; TCP only) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default

A newly created IPv4 ACL contains no rules.

Send comments to nx5000-docfeedback@cisco.com

If you do not specify a sequence number, the switch assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

IPv4 ACL configuration

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address network-wildcard

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address/prefix-len

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# deny udp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  switch(config-acl)# deny icmp host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

Send comments to nx5000-docfeedback@cisco.com

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply
- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements

Send comments to nx5000-docfeedback@cisco.com

- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time-exceeded messages
- **timestamp-reply**—Time-stamp replies
- **timestamp-request**—Time-stamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—EXEC (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (2)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

Send comments to nx5000-docfeedback@cisco.com

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—Unix-to-Unix Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

Send comments to nx5000-docfeedback@cisco.com

xdmcp—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network and a final rule that permits all other IPv4 traffic:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
remark	Configures a remark in an IPv4 ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.

Send comments to nx5000-docfeedback@cisco.com

deny (IPv6)

To create an IPv6 access control list (ACL) rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.To create an IPv6 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

no deny *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number* | **no**] **deny icmp** *source destination* [*icmp-message*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Internet Protocol v6

[*sequence-number*] **deny ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol

[*sequence-number* | **no**] **deny sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number* | **no**] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Send comments to nx5000-docfeedback@cisco.com

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **ahp—**Specifies that the rule applies to Authentication Header Protocol (AHP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **esp**—Specifies that the rule applies to Encapsulating Security Payload (ESP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ipv6**—Specifies that the rule applies to all IPv6 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **pcp**—Specifies that the rule applies to Payload Compression Protocol (PCP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **sctp**—Specifies that the rule applies to Stream Control Transmission Protocol (SCTP) traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

Send comments to nx5000-docfeedback@cisco.com

dscp *dscp*	(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **ef**—Expedited Forwarding (101110)
flow-label *flow-label-value*	(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575.
fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(ICMP only: Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under "ICMPv6 Message Types" in the "Usage Guidelines" section.

Send comments to nx5000-docfeedback@cisco.com

operator port [*port*]	(Optional; TCP, UDP, and SCTP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than the *port* argument. • **lt**—Matches only if the port in the packet is less than the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP, UDP, and SCTP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
flags	(TCP only; Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default None

Send comments to nx5000-docfeedback@cisco.com

Command Modes IPv6 ACL configuration

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv6-address/prefix-len

  This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

  ```
  switch(config-acl)# deny udp 2001:0db8:85a3::/48 any
  ```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv6-address*

  This syntax is equivalent to *IPv6-address*/128.

  This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

  ```
  switch(config-acl)# deny icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMPv6 Message Types

The *icmp-message* argument can be the ICMPv6 message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **beyond-scope**—Destination beyond scope
- **destination-unreachable**—Destination address is unreachable
- **echo-reply**—Echo reply
- **echo-request**—Echo request (ping)
- **header**—Parameter header problems

Send comments to nx5000-docfeedback@cisco.com

- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction
- **mld-report**—Multicast Listener Discovery Report
- **nd-na**—Neighbor discovery neighbor advertisements
- **nd-ns**—Neighbor discovery neighbor solicitations
- **next-header**—Parameter next header problems
- **no-admin**—Administration prohibited destination
- **no-route**—No route to destination
- **packet-too-big**—Packet too big
- **parameter-option**—Parameter option problems
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—Neighbor redirect
- **renum-command**—Router renumbering command
- **renum-result**—Router renumbering result
- **renum-seq-number**—Router renumbering sequence number reset
- **router-advertisement**—Neighbor discovery router advertisements
- **router-renumbering**—All router renumbering
- **router-solicitation**—Neighbor discovery router solicitations
- **time-exceeded**—All time exceeded messages
- **unreachable**—All unreachable

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **bgp**—Border Gateway Protocol (179)
- **chargen**—Character generator (19)
- **cmd**—Remote commands (rcmd, 514)
- **daytime**—Daytime (13)
- **discard**—Discard (9)
- **domain**—Domain Name Service (53)
- **drip**—Dynamic Routing Information Protocol (3949)
- **echo**—Echo (7)
- **exec**—Exec (rsh, 512)
- **finger**—Finger (79)
- **ftp**—File Transfer Protocol (21)

Send comments to nx5000-docfeedback@cisco.com

- **ftp-data**—FTP data connections (2)
- **gopher**—Gopher (7)
- **hostname**—NIC hostname server (11)
- **ident**—Ident Protocol (113)
- **irc**—Internet Relay Chat (194)
- **klogin**—Kerberos login (543)
- **kshell**—Kerberos shell (544)
- **login**—Login (rlogin, 513)
- **lpd**—Printer service (515)
- **nntp**—Network News Transport Protocol (119)
- **pim-auto-rp**—PIM Auto-RP (496)
- **pop2**—Post Office Protocol v2 (19)
- **pop3**—Post Office Protocol v3 (11)
- **smtp**—Simple Mail Transport Protocol (25)
- **sunrpc**—Sun Remote Procedure Call (111)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **telnet**—Telnet (23)
- **time**—Time (37)
- **uucp**—Unix-to-Unix Copy Program (54)
- **whois**—WHOIS/NICNAME (43)
- **www**—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **biff**—Biff (mail notification, comsat, 512)
- **bootpc**—Bootstrap Protocol (BOOTP) client (68)
- **bootps**—Bootstrap Protocol (BOOTP) server (67)
- **discard**—Discard (9)
- **dnsix**—DNSIX security protocol auditing (195)
- **domain**—Domain Name Service (DNS, 53)
- **echo**—Echo (7)
- **isakmp**—Internet Security Association and Key Management Protocol (5)
- **mobile-ip**—Mobile IP registration (434)
- **nameserver**—IEN116 name service (obsolete, 42)
- **netbios-dgm**—NetBIOS datagram service (138)
- **netbios-ns**—NetBIOS name service (137)

Send comments to nx5000-docfeedback@cisco.com

- **netbios-ss**—NetBIOS session service (139)
- **non500-isakmp**—Internet Security Association and Key Management Protocol (45)
- **ntp**—Network Time Protocol (123)
- **pim-auto-rp**—PIM Auto-RP (496)
- **rip**—Routing Information Protocol (router, in.routed, 52)
- **snmp**—Simple Network Management Protocol (161)
- **snmptrap**—SNMP Traps (162)
- **sunrpc**—Sun Remote Procedure Call (111)
- **syslog**—System Logger (514)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules denying all TCP and UDP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that denies all IPv6 traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# deny ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
remark	Configures a remark in an ACL.
time-range	Configures a time range.

Send comments to nx5000-docfeedback@cisco.com

deny (MAC)

To create a Media Access Control (MAC) access control list (ACL)+ rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
source	Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
protocol	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section.
cos *cos-value*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the class of service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7.
vlan *vlan-id*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the VLAN ID given. The *vlan-id* argument can be an integer from 1 to 4094.

Command Default

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the switch assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

MAC ACL configuration mode

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the switch applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

  ```
  MAC-address MAC-mask
  ```

  This example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  This example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

  ```
  switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. Protocol numbers are a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—EtherType 0x6000 (0x6000)
- **etype-8042**—EtherType 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)
- **vines-echo**—VINES Echo (0x0baf)

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with rules that permit any non-IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)# permit any any
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
permit (MAC)	Configures a deny rule in a MAC ACL.
remark	Configures a remark in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.

Send comments to nx5000-docfeedback@cisco.com

description (user role)

To configure a description for a user role, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text string that describes the user role. The maximum length is 128 alphanumeric characters.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can include blank spaces in the user role description text.

Examples

This example shows how to configure the description for a user role:

```
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

This example shows how to remove the description from a user role:

```
switch(config)# role name MyRole
switch(config-role)# no description
```

Related Commands

Command	Description
show role	Displays information about the user role configuration.

Send comments to nx5000-docfeedback@cisco.com

feature

To configure a feature in a user role feature group, use the **feature** command. To delete a feature in a user role feature group, use the **no** form of this command.

feature *feature-name*

no feature *feature-name*

Syntax Description

feature-name	Switch feature name as listed in the **show role feature** command output.

Command Default

None

Command Modes

User role feature group configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **show role** feature command to list the valid feature names to use in this command.

Examples

This example shows how to add features to a user role feature group:

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

This example shows how to remove a feature from a user role feature group:

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

Related Commands

Command	Description
role feature-group name	Creates or configures a user role feature group.
show role feature-group	Displays the user role feature groups.

Send comments to nx5000-docfeedback@cisco.com

interface policy deny

To enter interface policy configuration mode for a user role, use the **interface policy deny** command. To revert to the default interface policy for a user role, use the **no** form of this command.

interface policy deny

no interface policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enter interface policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

This example shows how to revert to the default interface policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

ip access-list

To create an IPv4 access control list (ACL) or to enter IP access list configuration mode for a specific ACL, use the **ip access-list** command. To remove an IPv4 ACL, use the **no** form of this command.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric characters long. The name cannot contain a space or quotation mark.

Command Default

No IPv4 ACLs are defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use IPv4 ACLs to filter IPv4 traffic.

When you use the **ip access-list** command, the switch enters IP access list configuration mode, where you can use the IPv4 **deny** and **permit** commands to configure rules for the ACL. If the specified ACL does not exist, the switch creates it when you enter this command.

Use the **ip access-group** command to apply the ACL to an interface.

Every IPv4 ACL has the following implicit rule as its last rule:

```
deny ip any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

IPv4 ACLs do not include additional implicit rules to enable the neighbor discovery process. The Address Resolution Protocol (ARP), which is the IPv4 equivalent of the IPv6 neighbor discovery process, uses a separate data link layer protocol. By default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Examples

This example shows how to enter IP access list configuration mode for an IPv4 ACL named ip-acl-01:

```
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
access-class	Applies an IPv4 ACL to a VTY line.
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-group	Applies an IPv4 ACL to an interface.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.

Send comments to nx5000-docfeedback@cisco.com

ip port access-group

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**

no ip port access-group *access-list-name* **in**

Syntax Description

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

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

By default, no IPv4 ACLs are applied to an interface.

You can use the **ip port access-group** command to apply an IPv4 ACL as a port ACL to the following interface types:

- Layer 2 Ethernet interfaces
- Layer 2 EtherChannel interfaces

You can also apply an IPv4 ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

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

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

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

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

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs.
show ip access-lists	Shows either a specific IPv4 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

Send comments to nx5000-docfeedback@cisco.com

ipv6 access-list

To create an IPv6 access control list (ACL) or to enter IP access list configuration mode for a specific ACL, use the **ipv6 access-list** command. To remove an IPv6 ACL, use the **no** form of this command.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv6 ACL, which can be up to 64 alphanumeric characters long. The name cannot contain a space or quotation mark.

Command Default

No IPv6 ACLs are defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

Use IPv6 ACLs to filter IPv6 traffic.

When you use the **ipv6 access-list** command, the switch enters IP access list configuration mode, where you can use the IPv6 **deny** and **permit** commands to configure rules for the ACL. If the specified ACL does not exist, the switch creates it when you enter this command.

Every IPv6 ACL has the following implicit rule as its last rule:

```
deny ipv6 any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

Examples

This example shows how to enter IP access list configuration mode for an IPv6 ACL named ipv6-acl-01:

```
switch(config)# ipv6 access-list ipv6-acl-01
switch(config-ipv6-acl)#
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.

Send comments to nx5000-docfeedback@cisco.com

ipv6 port traffic-filter

To apply an IPv6 access control list (ACL) to an interface as a port ACL, use the **ipv6 port traffic-filter** command. To remove an IPv6 ACL from an interface, use the **no** form of this command.

ipv6 port traffic-filter *access-list-name* **in**

no ipv6 port traffic-filter *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
in	Specifies that the device applies the ACL to inbound traffic.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

By default, no IPv6 ACLs are applied to an interface.

You can use the **ipv6 port traffic-filter** command to apply an IPv6 ACL as a port ACL to the following interface types:

- Ethernet interfaces
- EtherChannel interfaces

You can also use the **ipv6 port traffic-filter** command to apply an IPv6 ACL as a port ACL to the following interface types:

- VLAN interfaces

Note You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the **feature interface-vlan** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl to Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl in
```

This example shows how to remove an IPv6 ACL named ipv6-acl from Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl in
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs.
show ipv6 access-lists	Shows either a specific IPv6 ACL or all IPv6 ACLs.

Send comments to nx5000-docfeedback@cisco.com

mac access-list

To create a Media Access Control (MAC) access control list (ACL) or to enter MAC access list configuration mode for a specific ACL, use the **mac access-list** command. To remove a MAC ACL, use the **no** form of this command.

mac access-list *access-list-name*

no mac access-list *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACLACL, which can be up to 64 alphanumeric, case-sensitive characters long.

Command Default

No MAC ACLs are defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use MAC ACLs to filter non-IP traffic.

When you use the **mac access-list** command, the switch enters MAC access list configuration mode, where you can use the MAC **deny** and **permit** commands to configure rules for the ACL. If the ACL specified does not exist, the switch creates it when you enter this command.

Use the **mac access-group** command to apply the ACL to an interface.

Every MAC ACL has the following implicit rule as its last rule:

```
deny any any protocol
```

This implicit rule ensures that the switch denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

Examples

This example shows how to enter MAC access list configuration mode for a MAC ACL named mac-acl-01:

```
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac access-group	Applies a MAC ACL to an interface.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
permit (MAC)	Configures a permit rule in a MAC ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

Send comments to nx5000-docfeedback@cisco.com

mac port access-group

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

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters long.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

By default, no MAC ACLs are applied to an interface.

MAC ACLs apply to non-IP traffic.

You can use the **mac port access-group** command to apply a MAC ACL as a port ACL to the following interface types:

- Layer 2 interfaces
- Layer 2 EtherChannel interfaces

You can also apply a MAC ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies MAC ACLs only to inbound traffic. When the switch applies a MAC ACL, the switch checks packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply a MAC ACL named mac-acl-01 to Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
```

This example shows how to remove a MAC ACL named mac-acl-01 from Ethernet interface 1/2:

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

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs.
show mac access-lists	Shows either a specific MAC ACL or all MAC ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

Send comments to nx5000-docfeedback@cisco.com

match

To specify an access control list (ACL) for traffic filtering in a VLAN access map, use the **match** command. To remove a **match** command from a VLAN access map, use the **no** form of this command.

match {ip | ipv6 | mac} address *access-list-name*

no match {ip | ipv6 | mac} address *access-list-name*

Syntax Description

ip	Specifies an IPv4 ACL.
ipv6	Specifies an IPv6 ACL
mac	Specifies a MAC ACL.
address *access-list-name*	Specifies the IPv4, IPv6, or MAC address and the access list name. The name can be up to 64 alphanumeric, case-sensitive characters long.

Command Default

By default, the switch classifies traffic and applies IPv4 ACLs to IPv4 traffic and MAC ACLs to all other traffic.

Command Modes

VLAN access-map configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can specify only one **match** command per access map.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send comments to nx5000-docfeedback@cisco.com

permit (IPv4)

To create an IPv4 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **permit** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Internet Group Management Protocol

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Internet Protocol v4

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Transmission Control Protocol

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

Send comments to nx5000-docfeedback@cisco.com

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following: – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

Send comments to nx5000-docfeedback@cisco.com

dscp *dscp*	(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **ef**—Expedited Forwarding (101110)

Send comments to nx5000-docfeedback@cisco.com

precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical**—Precedence 5 (101) • **flash**—Precedence 3 (011) • **flash-override**—Precedence 4 (100) • **immediate**—Precedence 2 (010) • **internet**—Precedence 6 (110) • **network**—Precedence 7 (111) • **priority**—Precedence 1 (001) • **routine**—Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(Optional; IGMP only) Rule that matches only packets of the specified ICMP message type. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.
igmp-message	(Optional; IGMP only) Rule that matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace

Send comments to nx5000-docfeedback@cisco.com

operator port [*port*]	(Optional; TCP and UDP only) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than the *port* argument. • **lt**—Matches only if the port in the packet is less than the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
flags	(Optional; TCP only) Rule that matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(Optional; TCP only) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default A newly created IPv4 ACL contains no rules.

Send comments to nx5000-docfeedback@cisco.com

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

IPv4 ACL configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address network-wildcard

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address/prefix-len

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit udp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  switch(config-acl)# permit icmp host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

Send comments to nx5000-docfeedback@cisco.com

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply
- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements

Send comments to nx5000-docfeedback@cisco.com

- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time-exceeded messages
- **timestamp-reply**—Time-stamp replies
- **timestamp-request**—Time-stamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—EXEC (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (2)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

Send comments to nx5000-docfeedback@cisco.com

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—Unix-to-Unix Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

Send comments to nx5000-docfeedback@cisco.com

xdmcp—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-list	Configures an IPv4 ACL.
remark	Configures a remark in an ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.

Send comments to nx5000-docfeedback@cisco.com

permit (IPv6)

To create an IPv6 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

no permit *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number* | **no**] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Internet Protocol v6

[*sequence-number*] **permit ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol

[*sequence-number* | **no**] **permit sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Transmission Control Protocol

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number* | **no**] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Send comments to nx5000-docfeedback@cisco.com

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **ahp—**Specifies that the rule applies to Authentication Header Protocol (AHP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **esp**—Specifies that the rule applies to Encapsulating Security Payload (ESP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ipv6**—Specifies that the rule applies to all IPv6 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **pcp**—Specifies that the rule applies to Payload Compression Protocol (PCP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available. • **sctp**—Specifies that the rule applies to Stream Control Transmission Protocol (SCTP) traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

Send comments to nx5000-docfeedback@cisco.com

dscp *dscp*	(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **ef**—Expedited Forwarding (101110)
flow-label *flow-label-value*	(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575.
fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(ICMP only: Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under "ICMPv6 Message Types" in the "Usage Guidelines" section.

Send comments to nx5000-docfeedback@cisco.com

operator port [*port*]	(Optional; TCP, UDP, and SCTP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than the *port* argument. • **lt**—Matches only if the port in the packet is less than the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP, UDP, and SCTP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
flags	(TCP only; Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default None

Send comments to nx5000-docfeedback@cisco.com

Command Modes IPv6 ACL configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv6-address/prefix-len

  This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

  ```
  switch(config-acl)# permit udp 2001:0db8:85a3::/48 any
  ```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv6-address*

  This syntax is equivalent to *IPv6-address*/128.

  This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

  ```
  switch(config-acl)# permit icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMPv6 Message Types

The *icmp-message* argument can be the ICMPv6 message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **beyond-scope**—Destination beyond scope
- **destination-unreachable**—Destination address is unreachable
- **echo-reply**—Echo reply
- **echo-request**—Echo request (ping)
- **header**—Parameter header problems

Send comments to nx5000-docfeedback@cisco.com

- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction
- **mld-report**—Multicast Listener Discovery Report
- **nd-na**—Neighbor discovery neighbor advertisements
- **nd-ns**—Neighbor discovery neighbor solicitations
- **next-header**—Parameter next header problems
- **no-admin**—Administration prohibited destination
- **no-route**—No route to destination
- **packet-too-big**—Packet too big
- **parameter-option**—Parameter option problems
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—Neighbor redirect
- **renum-command**—Router renumbering command
- **renum-result**—Router renumbering result
- **renum-seq-number**—Router renumbering sequence number reset
- **router-advertisement**—Neighbor discovery router advertisements
- **router-renumbering**—All router renumbering
- **router-solicitation**—Neighbor discovery router solicitations
- **time-exceeded**—All time exceeded messages
- **unreachable**—All unreachable

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **bgp**—Border Gateway Protocol (179)
- **chargen**—Character generator (19)
- **cmd**—Remote commands (rcmd, 514)
- **daytime**—Daytime (13)
- **discard**—Discard (9)
- **domain**—Domain Name Service (53)
- **drip**—Dynamic Routing Information Protocol (3949)
- **echo**—Echo (7)
- **exec**—Exec (rsh, 512)
- **finger**—Finger (79)
- **ftp**—File Transfer Protocol (21)

Send comments to nx5000-docfeedback@cisco.com

- **ftp-data**—FTP data connections (2)
- **gopher**—Gopher (7)
- **hostname**—NIC hostname server (11)
- **ident**—Ident Protocol (113)
- **irc**—Internet Relay Chat (194)
- **klogin**—Kerberos login (543)
- **kshell**—Kerberos shell (544)
- **login**—Login (rlogin, 513)
- **lpd**—Printer service (515)
- **nntp**—Network News Transport Protocol (119)
- **pim-auto-rp**—PIM Auto-RP (496)
- **pop2**—Post Office Protocol v2 (19)
- **pop3**—Post Office Protocol v3 (11)
- **smtp**—Simple Mail Transport Protocol (25)
- **sunrpc**—Sun Remote Procedure Call (111)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **telnet**—Telnet (23)
- **time**—Time (37)
- **uucp**—Unix-to-Unix Copy Program (54)
- **whois**—WHOIS/NICNAME (43)
- **www**—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **biff**—Biff (mail notification, comsat, 512)
- **bootpc**—Bootstrap Protocol (BOOTP) client (68)
- **bootps**—Bootstrap Protocol (BOOTP) server (67)
- **discard**—Discard (9)
- **dnsix**—DNSIX security protocol auditing (195)
- **domain**—Domain Name Service (DNS, 53)
- **echo**—Echo (7)
- **isakmp**—Internet Security Association and Key Management Protocol (5)
- **mobile-ip**—Mobile IP registration (434)
- **nameserver**—IEN116 name service (obsolete, 42)
- **netbios-dgm**—NetBIOS datagram service (138)
- **netbios-ns**—NetBIOS name service (137)

Send comments to nx5000-docfeedback@cisco.com

- **netbios-ss**—NetBIOS session service (139)
- **non500-isakmp**—Internet Security Association and Key Management Protocol (45)
- **ntp**—Network Time Protocol (123)
- **pim-auto-rp**—PIM Auto-RP (496)
- **rip**—Routing Information Protocol (router, in.routed, 52)
- **snmp**—Simple Network Management Protocol (161)
- **snmptrap**—SNMP Traps (162)
- **sunrpc**—Sun Remote Procedure Call (111)
- **syslog**—System Logger (514)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules permitting all TCP and UDP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that permits all IPv6 traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 access-list	Configures an IPv6 ACL.
remark	Configures a remark in an ACL.

Send comments to nx5000-docfeedback@cisco.com

permit (MAC)

To create a MAC access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan vlan-id**]

no permit *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
source	Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
protocol	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section.
cos *cos-value*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7.
vlan *vlan-id*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the VLAN ID given. The *vlan-id* argument can be an integer from 1 to 4094.

Command Default

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the switch assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

MAC ACL configuration mode

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the switch applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

```
MAC-address MAC-mask
```

This example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

```
switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
```

This example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

```
switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—Ethertype 0x6000 (0x6000)
- **etype-8042**—Ethertype 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)
- **vines-echo**—VINES Echo (0x0baf)

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with a rule that permits all IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)#
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac access-list	Configures a MAC ACL.
remark	Configures a remark in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.

Send comments to nx5000-docfeedback@cisco.com

permit interface

To add interfaces for a user role interface policy, use the **permit interface** command. To remove interfaces, use the **no** form of this command.

permit interface *interface-list*

no permit interface

Syntax Description

interface-list	List of interfaces that the user role has permission to access.

Command Default

All interfaces

Command Modes

Interface policy configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

For permit interface statements to work, you need to configure a command rule to allow interface access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

Examples

This example shows how to configure a range of interfaces for a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
```

This example shows how to configure a list of interfaces for a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5
```

This example shows how to remove an interface from a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 1/2
```

Related Commands

Command	Description
interface policy deny	Enters interface policy configuration mode for a user role.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

permit vlan

To add VLANs for a user role VLAN policy, use the **permit vlan** command. To remove VLANs, use the **no** form of this command.

permit vlan *vlan-list*

no permit vlan

Syntax Description

vlan-list	List of VLANs that the user role has permission to access.

Command Default

All VLANs

Command Modes

VLAN policy configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

For **permit vlan** statements to work, you need to configure a command **rule** to allow VLAN access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

Examples

This example shows how to configure a range of VLANs for a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

This example shows how to configure a list of VLANs for a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

This example shows how to remove a VLAN from a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
vlan policy deny	Enters VLAN policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

permit vrf

To add virtual routing and forwarding instances (VRFs) for a user role VRF policy, use the **permit vrf** command. To remove VRFs, use the **no** form of this command.

permit vrf *vrf-list*

no permit vrf

Syntax Description

vrf-list	List of VRFs that the user role has permission to access.

Command Default

All VRFs

Command Modes

VRF policy configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure a range of VRFs for a user role VRF policy:

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

Related Commands

Command	Description
vrf policy deny	Enters VRF policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

permit vsan

To permit access to a VSAN policy for a user role, use the **permit vsan** command. To revert to the default VSAN policy configuration for a user role, use the **no** form of this command.

permit vsan *vsan-list*

no permit vsan *vsan-list*

Syntax Description

vsan-list	Range of VSANs accessible to a user role. The range is from 1 to 4093. You can separate the range using the following separators: • **,** is a multirange separator; for example, 1-5, 10, 12, 100-201. • **-** is a range separator; for example, 101-201.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is enabled only after you deny a VSAN policy by using the **vsan policy deny** command.

Examples

This example shows how to permit access to a VSAN policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# permit vsan 10, 12, 100-104
switch(config-role-vsan)#
```

Related Commands

Command	Description
vsan policy deny	Denies access to a VSAN policy for a user.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a Cisco Nexus 5000 Series switch, use the **radius-server deadtime** command. To revert to the default, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Command Default

0 minutes

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The dead-time interval is the number of minutes before the switch checks a RADIUS server that was previously unresponsive.

Note When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to configure the global dead-time interval for all RADIUS servers to perform periodic monitoring:

```
switch(config)# radius-server deadtime 5
```

This example shows how to revert to the default for the global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
switch(config)# no radius-server deadtime 5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send comments to nx5000-docfeedback@cisco.com

radius-server directed-request

To allow users to send authentication requests to a specific RADIUS server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured RADIUS server group.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can specify the *username@vrfname*:*hostname* during login, where *vrfname* is the VRF to use and *hostname* is the name of a configured RADIUS server. The username is sent to the RADIUS server for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific RADIUS server when logging in:

```
switch(config)# radius-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific RADIUS server when logging in:

```
switch(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server directed-request	Displays the directed request RADIUS server configuration.

Send comments to nx5000-docfeedback@cisco.com

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	RADIUS server IPv6 address in the *X:X:X:X* format.
key	(Optional) Configures the RADIUS server preshared secret key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.
pac	(Optional) Enables the generation of Protected Access Credentials on the RADIUS Cisco ACS server for use with Cisco TrustSec.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

Send comments to nx5000-docfeedback@cisco.com

username *name*	Specifies a username in the test packets. The is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the range is from 1 to 60 seconds.

Command Default

Accounting port: 1813

Authentication port: 1812

Accounting: enabled

Authentication: enabled

Retransmission count: 1

Idle-time: 0

Server monitoring: disabled

Timeout: 5 seconds

Test username: test

Test password: test

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to configure RADIUS server authentication and accounting parameters:

```
switch(config)# radius-server host 192.168.2.3 key HostKey
switch(config)# radius-server host 192.168.2.3 auth-port 2003
switch(config)# radius-server host 192.168.2.3 acct-port 2004
switch(config)# radius-server host 192.168.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 192.168.2.3 test idle-time 10
switch(config)# radius-server host 192.168.2.3 test username tester
switch(config)# radius-server host 192.168.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send comments to nx5000-docfeedback@cisco.com

radius-server key

To configure a RADIUS shared secret key, use the **radius-server key** command. To remove a configured shared secret, use the **no** form of this command.

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key used to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.

Command Default

Clear text authentication

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **radius-server host** command.

Examples

This example shows how to provide various scenarios to configure RADIUS authentication:

```
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send comments to nx5000-docfeedback@cisco.com

radius-server retransmit

To specify the number of times that the switch should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to the default, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times.

Command Default

1 retransmission

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure the number of retransmissions to RADIUS servers:

```
switch(config)# radius-server retransmit 3
```

This example shows how to revert to the default number of retransmissions to RADIUS servers:

```
switch(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send comments to nx5000-docfeedback@cisco.com

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. To revert to the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Command Default

1 second

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure the timeout interval:

```
switch(config)# radius-server timeout 30
```

This example shows how to revert to the default interval:

```
switch(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send comments to nx5000-docfeedback@cisco.com

remark

To enter a comment into an IPv4 or MAC access control list (ACL), use the **remark** command. To remove a remark command, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

Syntax Description

sequence-number	(Optional) Sequence number of the **remark** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. This argument can be up to 100 characters.

Command Default

No ACL contains a remark by default.

Command Modes

IPv4 ACL configuration mode

MAC ACL configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the switch accepts the first 100 characters and drops any additional characters.

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.

Send comments to nx5000-docfeedback@cisco.com

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name starting-number increment*

resequence time-range *time-range-name starting-number increment*

Syntax Description

access-list-type	Type of the ACL. Valid values for this argument are the following keywords: • **arp** • **ip** • **mac**
access-list *access-list-name*	Specifies the name of the ACL.
time-range *time-range-name*	Specifies the name of the time range.
starting-number	Sequence number for the first rule in the ACL or time range.
increment	Number that the switch adds to each subsequent sequence number.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL or time range. The new sequence number for the first rule is determined by the *starting-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, then no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch(config)# show ip access-lists ip-acl-01
```

Send comments to nx5000-docfeedback@cisco.com

```
IP access list ip-acl-01
        7 permit tcp 128.0.0.0/16 any eq www
        10 permit udp 128.0.0.0/16 any
        13 permit icmp 128.0.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp 128.0.0.0/16 any eq www
        110 permit udp 128.0.0.0/16 any
        120 permit icmp 128.0.0.0/16 any eq echo
        130 deny igmp any any
switch(config)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

Send comments to nx5000-docfeedback@cisco.com

role feature-group name

To create or specify a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description

group-name	User role feature group name. The *group-name* has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch(config)# no role feature-group name MyGroup
switch(config)#
```

Related Commands

Command	Description
feature-group name	Specifies or creates a user role feature group and enters user role feature group configuration mode.
show role feature-group	Displays the user role feature groups.

Send comments to nx5000-docfeedback@cisco.com

role name

To create or specify a user role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name *role-name*

no role name *role-name*

Syntax Description

role-name	User role name. The *role-name* has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

A Cisco Nexus 5000 Series switch provides the following default user roles:

- Network Administrator—Complete read-and-write access to the entire switch
- Complete read access to the entire switch

You cannot change or remove the default user roles.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to remove a user role:

```
switch(config)# no role name MyRole
```

Related Commands

Command	Description
show role	Displays the user roles.

Send comments to nx5000-docfeedback@cisco.com

rule

To configure rules for a user role, use the **rule** command. To delete a rule, use the **no** form of this command.

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

Syntax Description

number	Sequence number for the rule. The switch applies the rule with the highest value first and then the rest in descending order.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command *command-string*	Specifies a command string.
read	Specifies read access.
read-write	Specifies read and write access.
feature *feature-name*	(Optional) Specifies a feature name. Use the **show role feature** command to list the switch feature names.
feature-group *group-name*	(Optional) Specifies a feature group.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Examples

This example shows how to add rules to a user role:

```
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to remove rule from a user role:

```
switch(config)# role MyRole
switch(config-role)# no rule 10
```

Related Commands

Command	Description
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.

Send comments to nx5000-docfeedback@cisco.com

server

To add a server to a RADIUS or TACACS+ server group, use the **server** command. To delete a server from a server group, use the **no** form of this command.

server {*ipv4-address* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X*:*X*:*X*::*X* format.
hostname	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

RADlUS server group configuration mode

TACACS+ server group configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure up to 64 servers in a server group.

Use the **aaa group server radius** command to enter RADIUS server group configuration mode or **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

Note You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to add a server to a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.1.1
```

This example shows how to delete a server from a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.1.1
```

This example shows how to add a server to a TACACS+ server group:

```
switch(config)# feature tacacs+
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 192.168.2.2
```

This example shows how to delete a server from a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 192.168.2.2
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

Send comments to nx5000-docfeedback@cisco.com

show aaa accounting

To display authentication, authorization, and accounting (AAA) accounting configuration, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configuration of the accounting log:

```
switch# show aaa accounting
```

Related Commands

Command	Description
aaa accounting default	Configures AAA methods for accounting.

Send comments to nx5000-docfeedback@cisco.com

show aaa authentication

To display authentication, authorization, and accounting (AAA) authentication configuration information, use the **show aaa authentication** command.

show aaa authentication login [**error-enable** | **mschap**]

Syntax Description

error-enable	(Optional) Displays the authentication login error message enable configuration.
mschap	(Optional) Displays the authentication login Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) enable configuration.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured authentication parameters:

```
switch# show aaa authentication
```

This example shows how to display the authentication login error enable configuration:

```
switch# show aaa authentication login error-enable
```

This example shows how to display the authentication login MS-CHAP configuration:

```
switch# show aaa authentication login mschap
```

Related Commands

Command	Description
aaa authentication	Configures AAA authentication methods.

Send comments to nx5000-docfeedback@cisco.com

show aaa authorization

To display AAA authorization configuration information, use the **show aaa authorization** command.

show aaa authorization [**all**]

Syntax Description

all	(Optional) Displays configured and default values.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the configured authorization methods:

```
switch# show aaa authorization
AAA command authorization:
         default authorization for config-commands: none

switch#
```

This example shows how to revert to the default AAA authorization methods for configuration commands:

```
switch(config)# no aaa authorization config-commands default group TacGroup local
switch(config)#
```

Related Commands

Command	Description
aaa authorization commands default	Configures default AAA authorization methods for EXEC commands.
aaa authorization config-commands default	Configures default AAA authorization methods for configuration commands.

Send comments to nx5000-docfeedback@cisco.com

show aaa groups

To display authentication, authorization, and accounting (AAA) server group configuration, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display AAA group information:

```
switch# show aaa groups
```

Related Commands

Command	Description
aaa group server radius	Creates a RADIUS server group.

Send comments to nx5000-docfeedback@cisco.com

show aaa user

To display the status of the default role assigned by the authentication, authorization, and accounting (AAA) server administrator for remote authentication, use the **show aaa user** command.

show aaa user default-role

Syntax Description

default-role	Displays the status of the default AAA role.

Command Default

None

Command Modes

EXEC mode.

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the status of the default role assigned by the AAA server administrator for remote authentication:

```
switch# show aaa user default-role
enabled
switch#
```

Related Commands

Command	Description
aaa user default-role	Configures the default user for remote authentication.
show aaa authentication	Displays AAA authentication information.

Send comments to nx5000-docfeedback@cisco.com

show access-lists

To display all IPv4 and MAC access control lists (ACLs) or a specific ACL, use the **show access-lists** command.

show access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

The switch shows all ACLs unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all IPv4 and MAC ACLs on the switch:

```
switch# show access-lists
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

Send comments to nx5000-docfeedback@cisco.com

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size*] [**start-time** *year month day HH*:*MM*:*SS*] [**end-time** *year month day HH*:*MM*:*SS*]

Syntax Description

size	(Optional) Amount of the log to display in bytes. The range is from 0 to 250000.
start-time *year month day HH*:*MM*:*SS*	(Optional) Specifies a start time. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in standard 24-hour format.
end-time *year month day HH*:*MM*:*SS*	(Optional) Specifies an end time. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in standard 24-hour format.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the entire accounting log:

```
switch# show accounting log
```

This example shows how to display 400 bytes of the accounting log:

```
switch# show accounting log 400
```

This example shows how to display the accounting log starting at 16:00:00 on February 16, 2008:

```
switch# show accounting log start-time 2008 Feb 16 16:00:00
```

This example shows how to display the accounting log starting at 15:59:59 on February 1, 2008 and ending at 16:00:00 on February 29, 2008:

```
switch# show accounting log start-time 2008 Feb 1 15:59:59 end-time 2008 Feb 29 16:00:00
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

Send comments to nx5000-docfeedback@cisco.com

show ip access-lists

To display all IPv4 access control lists (ACLs) or a specific IPv4 ACL, use the **show ip access-lists** command.

show ip access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

The switch shows all IPv4 ACLs unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

By default, this command displays the IPv4 ACLs configured on the switch. The command displays the statistics information for an IPv4 ACL only if the IPv4 ACL is applied to the management (mgmt0) interface. If the ACL is applied to an SVI interface or in a QoS class map, then the command does not display any statistics information.

Examples

This example shows how to display all IPv4 ACLs on the switch:

```
switch# show ip access-lists

IP access list BulkData
        10 deny ip any any
IP access list CriticalData
        10 deny ip any any
IP access list Scavenger
        10 deny ip any any
IP access list deny
        10 deny ip 192.168.30.1/32 192.168.40.1/32
IP access list deny4
IP access list denyv4
        statistics per-entry
        20 deny ip 192.168.10.0/24 10.20.10.0/24 fragments
        30 permit udp 192.168.10.0/24 gt isakmp 192.168.20.0/24 lt 400
        40 permit icmp any any router-advertisement
        60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
        70 permit igmp any any host-report
        80 deny tcp any any rst
        90 deny tcp any any ack
        100 permit tcp any any fin
        110 permit tcp any gt 300 any lt 400
        130 deny tcp any range 200 300 any lt 600
```

Send comments to nx5000-docfeedback@cisco.com

```
IP access list dot
--More--
<--output truncated-->
switch#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

Send comments to nx5000-docfeedback@cisco.com

show ip arp

To display the Address Resolution Protocol (ARP) table statistics, use the **show ip arp** command.

show ip arp [**detail** | **vlan** *vlan-id* [**vrf** {*vrf-name* | **all** | **default** | **management**}]]

Syntax Description

detail	(Optional) Displays the detailed ARP information.
vlan *vlan-id*	(Optional) Displays the ARP information for a specified VLAN. The range is from 1 to 4094, except for the VLANs reserved for internal use.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) to use.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters, and is case sensitive.
all	Displays all VRF entries for the specified VLAN in the ARP table.
default	Displays the default VRF entry for the specified VLAN.
management	Displays the management VRF entry for the specified VLAN.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the ARP table:

```
switch# show ip arp

IP ARP Table for context default
Total number of entries: 1
Address         Age       MAC Address     Interface
90.10.10.2      00:03:11  000d.ece7.df7c  Vlan900
switch#
```

This example shows how to display the detailed ARP table:

```
switch# show ip arp detail

IP ARP Table for context default
Total number of entries: 1
Address         Age       MAC Address     Interface        Physical Interface
90.10.10.2      00:02:55  000d.ece7.df7c  Vlan900          Ethernet1/12
switch#
```

This example shows how to display the ARP table for VLAN 10 and all VRFs:

```
switch# show ip arp vlan 10 vrf all
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
clear ip arp	Clears the ARP cache and table.
show running-config arp	Displays the running ARP configuration.

Send comments to nx5000-docfeedback@cisco.com

show ipv6 access-lists

To display all IPv6 access control lists (ACLs) or a specific IPv6 ACL, use the **show ipv6 access-lists** command.

show ipv6 access-lists [*access-list-name*] [**expanded** | **summary**]

Syntax Description

access-list-name	(Optional) Name of an IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of IPv6 address groups or port groups show rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the "Usage Guidelines" section.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The device shows all IPv6 ACLs, unless you use the access-list-name argument to specify an ACL.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics is configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The show ipv6 access-lists command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the statistics per-entry command.
- The ACL is applied to an interface that is administratively up.

Examples

This example shows how to display all IPv6 ACLs on a switch:

```
switch# show ipv6 access-lists
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.

Send comments to nx5000-docfeedback@cisco.com

show mac access-lists

To display all Media Access Control (MAC) access control lists (ACLs) or a specific MAC ACL, use the **show mac access-lists** command.

show mac access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of a MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

The switch shows all MAC ACLs unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all MAC ACLs on the switch:

```
switch# show mac access-lists
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.

Send comments to nx5000-docfeedback@cisco.com

show radius-server

To display RADIUS server information, use the **show radius-server** command.

show radius-server [*hostname* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** [*group-name*] | **sorted | statistics** *hostname* | *ipv4-address* | *ipv6-address*]

Syntax Description

hostname	(Optional) RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	(Optional) RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) RADIUS server IPv6 address in the *X*:*X*::*X*:*X* format.
directed-request	(Optional) Displays the directed request configuration.
groups [*group-name*]	(Optional) Displays information about the configured RADIUS server groups. Supply a *group-name* to display information about a specific RADIUS server group.
sorted	(Optional) Displays sorted-by-name information about the RADIUS servers.
statistics	(Optional) Displays RADIUS statistics for the RADIUS servers. A hostname or IP address is required.

Command Default

Displays the global RADIUS server configuration.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

RADIUS preshared keys are not visible in the **show radius-server** command output. Use the **show running-config radius** command to display the RADIUS preshared keys.

Examples

This example shows how to display information for all RADIUS servers:

```
switch# show radius-server
```

This example shows how to display information for a specified RADIUS server:

```
switch# show radius-server 192.168.1.1
```

This example shows how to display the RADIUS directed request configuration:

```
switch# show radius-server directed-request
```

This example shows how to display information for RADIUS server groups:

```
switch# show radius-server groups
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display information for a specified RADIUS server group:

```
switch# show radius-server groups RadServer
```

This example shows how to display sorted information for all RADIUS servers:

```
switch# show radius-server sorted
```

This example shows how to display statistics for a specified RADIUS servers:

```
switch# show radius-server statistics 192.168.1.1
```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

Send comments to nx5000-docfeedback@cisco.com

show role

To display the user role configuration, use the **show role** command.

show role [**name** *role-name*]

Syntax Description		
	name *role-name*	(Optional) Displays information for a specific user role name.

Command Default Displays information for all user roles.

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display information for a specific user role:

```
switch# show role name MyRole
```

This example shows how to display information for all user roles:

```
switch# show role
```

Related Commands	Command	Description
	role name	Configures user roles.

Send comments to nx5000-docfeedback@cisco.com

show role feature

To display the user role features, use the **show role feature** command.

show role feature [**detail** | **name** *feature-name*]

Syntax Description

detail	(Optional) Displays detailed information for all features.
name *feature-name*	(Optional) Displays detailed information for a specific feature.

Command Default

Displays a list of user role feature names.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the user role features:

```
switch# show role feature
```

This example shows how to display detailed information all the user role features:

```
switch# show role feature detail
```

This example shows how to display detailed information a specific user role feature:

```
switch# show role feature name boot-variable
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

Send comments to nx5000-docfeedback@cisco.com

show role feature-group

To display the user role feature groups, use the **show role feature-group** command.

show role feature-group [**detail** | **name** *group-name*]

Syntax Description

detail	(Optional) Displays detailed information for all feature groups.
name *group-name*	(Optional) Displays detailed information for a specific feature group.

Command Default

Displays a list of user role feature groups.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the user role feature groups:

```
switch# show role feature-group
```

This example shows how to display detailed information about all the user role feature groups:

```
switch# show role feature-group detail
```

This example shows how to display information for a specific user role feature group:

```
switch# show role feature-group name SecGroup
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

Send comments to nx5000-docfeedback@cisco.com

show running-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the running configuration, use the **show running-config aaa** command.

show running-config aaa [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured AAA information in the running configuration:

```
switch# show running-config aaa
```

Send comments to nx5000-docfeedback@cisco.com

show running-config radius

To display RADIUS server information in the running configuration, use the **show running-config radius** command.

show running-config radius [**all**]

Syntax Description

all	(Optional) Displays default RADIUS configuration information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display information for RADIUS in the running configuration:

```
switch# show running-config radius
```

Related Commands

Command	Description
show radius-server	Displays RADIUS information.

Send comments to nx5000-docfeedback@cisco.com

show running-config security

To display user account, Secure Shell (SSH) server, and Telnet server information in the running configuration, use the **show running-config security** command.

show running-config security [**all**]

Syntax Description

all	(Optional) Displays default user account, SSH server, and Telnet server configuration information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display user account, SSH server, and Telnet server information in the running configuration:

```
switch# show running-config security
```

Send comments to nx5000-docfeedback@cisco.com

show ssh key

To display the Secure Shell (SSH) server key, use the **show ssh key** command.

show ssh key

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is available only when SSH is enabled using the **ssh server enable** command.

Examples

This example shows how to display the SSH server key:

```
switch# show ssh key
```

Related Commands

Command	Description
ssh server key	Configures the SSH server key.

Send comments to nx5000-docfeedback@cisco.com

show ssh server

To display the Secure Shell (SSH) server status, use the **show ssh server** command.

show ssh server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the SSH server status:

```
switch# show ssh server
```

Related Commands

Command	Description
ssh server enable	Enables the SSH server.

Send comments to nx5000-docfeedback@cisco.com

show startup-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the startup configuration, use the **show startup-config aaa** command.

show startup-config aaa

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the AAA information in the startup configuration:

```
switch# show startup-config aaa
```

Send comments to nx5000-docfeedback@cisco.com

show startup-config radius

To display RADIUS configuration information in the startup configuration, use the **show startup-config radius** command.

show startup-config radius

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the RADIUS information in the startup configuration:

```
switch# show startup-config radius
```

Send comments to nx5000-docfeedback@cisco.com

show startup-config security

To display user account, Secure Shell (SSH) server, and Telnet server configuration information in the startup configuration, use the **show startup-config security** command.

show startup-config security

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the user account, SSH server, and Telnet server information in the startup configuration:

```
switch# show startup-config security
```

Send comments to nx5000-docfeedback@cisco.com

show tacacs-server

To display TACACS+ server information, use the **show tacacs-server** command.

show tacacs-server [*hostname* | *ip4-address* | *ip6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

hostname	(Optional) TACACS+ server Domain Name Server (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) TACACS+ server IPv6 address in the *X:X:X::X* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured TACACS+ server groups.
sorted	(Optional) Displays sorted-by-name information about the TACACS+ servers.
statistics	(Optional) Displays TACACS+ statistics for the TACACS+ servers.

Defaults

Displays the global TACACS+ server configuration.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

TACACS+ preshared keys are not visible in the **show tacacs-server** command output. Use the **show running-config tacacs+** command to display the TACACS+ preshared keys.

You must use the **feature tacacs+** command before you can display TACACS+ information.

Examples

This example shows how to display information for all TACACS+ servers:

```
switch# show tacacs-server
```

This example shows how to display information for a specified TACACS+ server:

```
switch# show tacacs-server 192.168.2.2
```

This example shows how to display the TACACS+ directed request configuration:

```
switch# show tacacs-server directed-request
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display information for TACACS+ server groups:

```
switch# show tacacs-server groups
```

This example shows how to display information for a specified TACACS+ server group:

```
switch# show tacacs-server groups TacServer
```

This example shows how to display sorted information for all TACACS+ servers:

```
switch# show tacacs-server sorted
```

This example shows how to display statistics for a specified TACACS+ server:

```
switch# show tacacs-server statistics 192.168.2.2
```

Related Commands

Command	Description
show running-config tacacs+	Displays the TACACS+ information in the running configuration file.

Send comments to nx5000-docfeedback@cisco.com

show telnet server

To display the Telnet server status, use the **show telnet server** command.

show telnet server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the Telnet server status:

```
switch# show telnet server
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

Send comments to nx5000-docfeedback@cisco.com

show user-account

To display information about the user accounts on the switch, use the **show user-account** command.

show show user-account [*name*]

Syntax Description		
	name	(Optional) Information about the specified user account only.

Command Default Displays information about all the user accounts defined on the switch.

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display information about all the user accounts defined on the switch:

```
switch# show user-account
```

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

```
switch# show user-account admin
```

Send comments to nx5000-docfeedback@cisco.com

show users

To display the users currently logged on the switch, use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all the users currently logged on the switch:

```
switch# show users
```

Related Commands

Command	Description
clear user	Logs out a specific user.
username	Creates and configures a user account.

Send comments to nx5000-docfeedback@cisco.com

show vlan access-list

To display the contents of the IPv4 access control list (ACL) or MAC ACL associated with a specific VLAN access map, use the **show vlan access-list** command.

show vlan access-list *map-name*

Syntax Description

map-name	VLAN access list to show.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

For the specified VLAN access map, the switch displays the access map name and the contents of the ACL associated with the map.

Examples

This example shows how to display the contents of the ACL associated with the specified VLAN access map:

```
switch# show vlan access-list vlan1map
```

Related Commands

Command	Description
ip access-list	Create or configures an IPv4 ACL.
mac access-list	Create or configures a MAC ACL.
show access-lists	Displays information about how a VLAN access map is applied.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
vlan access-map	Configures a VLAN access map.

Send comments to nx5000-docfeedback@cisco.com

show vlan access-map

To display all VLAN access maps or a VLAN access map, use the **show vlan access-map** command.

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) VLAN access map to show.

Command Default

The switch shows all VLAN access maps, unless you use the *map-name* argument to select a specific access map.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

For each VLAN access map displayed, the switch shows the access map name, the ACL specified by the **match** command, and the action specified by the **action** command.

Use the **show vlan filter** command to see which VLANs have a VLAN access map applied to them.

Examples

This example shows how to display a specific VLAN access map:

```
switch# show vlan access-map vlan1map
```

This example shows how to display all VLAN access maps:

```
switch# show vlan access-map
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send comments to nx5000-docfeedback@cisco.com

show vlan filter

To display information about instances of the **vlan filter** command, including the VLAN access map and the VLAN IDs affected by the command, use the **show vlan filter** command.

show vlan filter [**access-map** *map-name* | **vlan** *vlan-id*]

Syntax Description

access-map *map-name*	(Optional) Limits the output to VLANs that the specified access map is applied to.
vlan *vlan-id*	(Optional) Limits the output to access maps that are applied to the specified VLAN only.

Command Default

All instances of VLAN access maps applied to a VLAN are displayed, unless you use the **access-map** keyword and specify an access map or you use the **vlan** keyword and specify a VLAN ID.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all VLAN access map information on the switch:

```
switch# show vlan filter
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send comments to nx5000-docfeedback@cisco.com

ssh

To create a Secure Shell (SSH) session using IPv4, use the **ssh** command.

ssh [*username@*]{*ipv4-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

username	(Optional) Username for the SSH session. The user name is not case sensitive, and has a maximum of 64 characters.
ipv4-address	IPv4 address of the remote host.
hostname	Hostname of the remote host. The hostname is case sensitive, and has a maximum of 64 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The name can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Default VRF

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to start an SSH session using IPv4:

```
switch# ssh 192.168.1.1 vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh server enable	Enables the SSH server.
ssh6	Starts an SSH session using IPv6 addressing.

Send comments to nx5000-docfeedback@cisco.com

ssh6

To create a Secure Shell (SSH) session using IPv6, use the **ssh6** command.

ssh6 [*username@*]{*ipv6-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive, and has a maximum of 64 characters.
ipv6-address	IPv6 address of the remote host.
hostname	Hostname of the remote host. The hostname is case sensitive, and has a maximum of 64 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH IPv6 session. The name can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Default VRF

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to start an SSH session using IPv6:

```
switch# ssh6 2001:0DB8::200C:417A vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh	Starts an SSH session using IPv4 addressing.
ssh server enable	Enables the SSH server.

Send comments to nx5000-docfeedback@cisco.com

ssh key

To create a Secure Shell (SSH) server key, use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies the Digital System Algrorithm (DSA) SSH server key.
force	(Optional) Forces the generation of a DSA SSH key even if previous ones are present.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048.

Command Default

1024-bit length

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

Examples

This example shows how to create an SSH server key using RSA with the default key length:

```
switch(config)# ssh key rsa
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch(config)# ssh key rsa 768
```

This example shows how to replace an SSH server key using DSA with the force option:

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

This example shows how to remove the DSA SSH server key:

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
ssh server enable	Enables the SSH server.

Send comments to nx5000-docfeedback@cisco.com

ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to enable the SSH server:

```
switch(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
switch(config)# no ssh server enable
```

Related Commands

Command	Description
show ssh server	Displays the SSH server key information.

Send comments to nx5000-docfeedback@cisco.com

storm-control level

To set the suppression level for traffic storm control, use the **storm-control level** command. To turn off the suppression mode or revert to the default, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*]

no storm-control {**broadcast** | **multicast** | **unicast**} **level**

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
level *percentage*	Specifies the percentage of the suppression level. The range is from 0 to 100 percent.
fraction	(Optional) Fraction of the suppression level. The range is from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

The period (.) is required when you enter the fractional-suppression level.

The suppression level is a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port.

Use the **show interfaces counters storm-control** command to display the discard count.

Use one of the following methods to turn off suppression for the specified traffic type:

- Set the level to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Examples

This example shows how to enable suppression of broadcast traffic and set the suppression threshold level:

```
switch(config-if)# storm-control broadcast level 30
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to disable the suppression mode for multicast traffic:

```
switch(config-if)# no storm-control multicast level
```

Related Commands

Command	Description
show interface	Displays the storm-control suppression counters for an interface.
show running-config	Displays the configuration of the interface.

Send comments to nx5000-docfeedback@cisco.com

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

time	Time interval in minutes. The range is from 1 to 1440.

Command Default

0 minutes

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to configure the dead-time interval and enable periodic monitoring:

```
switch(config)# tacacs-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch(config)# no tacacs-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive RADIUS or TACACS+ server group.
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

Send comments to nx5000-docfeedback@cisco.com

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **tacacs-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured TACACS+ server groups.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

During login, the user can specify the *username@vrfname*:*hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server. The username is sent to the server name for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch(config)# tacacs-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch(config)# no tacacs-server directed-request
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

Send comments to nx5000-docfeedback@cisco.com

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command. To revert to the defaults, use the **no** form of this command.

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

Syntax Description

hostname	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	TACACS+ server IPv6 address in the *X:X:X::X* format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout *seconds*	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Command Default

Idle time: disabled.

Server monitoring: disabled.

Timeout: 1 second.

Send comments to nx5000-docfeedback@cisco.com

Test username: test.

Test password: test.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

This example shows how to configure TACACS+ server host parameters:

```
switch(config)# tacacs-server host 192.168.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 192.168.2.3 test idle-time 10
switch(config)# tacacs-server host 192.168.2.3 test username tester
switch(config)# tacacs-server host 192.168.2.3 test password 2B9ka5
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

Send comments to nx5000-docfeedback@cisco.com

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To remove a configured shared secret, use the **no** form of this command.

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to display configure TACACS+ server shared keys:

```
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

Send comments to nx5000-docfeedback@cisco.com

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Seconds between retransmissions to the TACACS+ server. The valid range is 1 to 60 seconds.

Command Default

1 second

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to configure the TACACS+ server timeout value:

```
switch(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch(config)# no tacacs-server timeout 3
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

Send comments to nx5000-docfeedback@cisco.com

telnet

To create a Telnet session using IPv4 on a Cisco Nexus 5000 Series switch, use the **telnet** command.

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

ipv4-address	IPv4 address of the remote switch.
hostname	Hostname of the remote switch. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Port 23 is the default port.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To create a Telnet session with IPv6 addressing, use the **telnet6** command.

Examples

This example shows how to start a Telnet session using IPv4:

```
switch# telnet 192.168.1.1 vrf management
switch#
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet server enable	Enables the Telnet server.
telnet6	Creates a Telnet session using IPv6 addressing.

Send comments to nx5000-docfeedback@cisco.com

telnet server enable

To enable the Telnet server, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enable

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable the Telnet server:

```
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch(config)# no telnet server enable
```

Related Commands

Command	Description
show telnet server	Displays the Telnet server status.

Send comments to nx5000-docfeedback@cisco.com

telnet6

To create a Telnet session using IPv6 on the Cisco NX-OS switch, use the **telnet6** command.

telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

ipv6-address	IPv6 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Port 23 is the default port. The default VRF is used.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **telnet server enable** command.

To create a Telnet session with IPv4 addressing, use the **telnet** command.

Examples

This example shows how to start a Telnet session using an IPv6 address:

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
switch#
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet	Creates a Telnet session using IPv4 addressing.
telnet server enable	Enables the Telnet server.

Send comments to nx5000-docfeedback@cisco.com

use-vrf

To specify a virtual routing and forwarding instance (VRF) instance for a RADIUS or TACACS+ server group, use the **use-vrf** command. To remove the VRF instance, use the **no** form of this command.

use-vrf {*vrf-name* | **default** | **management**}

no use-vrf {*vrf-name* | **default** | **management**}

Syntax Description

vrf-name	VRF instance name. The name is case sensitive, and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

RADlUS server group configuration mode

TACACS+ server group configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

Use the **aaa group server radius** command RADIUS server group configuration mode or the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to specify a VRF instance for a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf management
```

This example shows how to specify a VRF instance for a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf management
```

This example shows how to remove the VRF instance from a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf management
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server information.
show tacacs-server groups	Displays TACACS+ server information.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.

Send comments to nx5000-docfeedback@cisco.com

username

To create and configure a user account, use the **username** command. To remove a user account, use the **no** form of this command.

username *user-id* [**expire** *date*] [**password** *password*] [**role** *role-name*]

username *user-id* **sshkey** {*key* | **filename** *filename*}

no username *user-id*

Syntax Description

user-id	User identifier for the user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. **Note** The Cisco NX-OS software does not allowed the "#" and "@" characters in the *user-id* argument text string.
expire *date*	(Optional) Specifies the expire date for the user account. The format for the *date* argument is YYYY-MM-DD.
password *password*	(Optional) Specifies a password for the account. The default is no password. **Note** Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>).
role *role-name*	(Optional) Specifies the role which the user is to be assigned to.
sshkey	(Optional) Specifies an SSH key for the user account.
key	SSH key string.
filename *filename*	Specifies the name of a file that contains the SSH key string.

Command Default

No expiration date, password, or SSH key.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch accepts only strong passwords. The characteristics of a strong password include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as "abcd")
- Does not contain many repeating characters (such as "aaabbb")
- Does not contain dictionary words

Send comments to nx5000-docfeedback@cisco.com

- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

Examples

This example shows how to create a user account with a password:

```
switch(config)# username user1 password Ci5co321
```

This example shows how to configure the SSH key for a user account:

```
switch(config)# username user1 sshkey file bootflash:key_file
```

Related Commands

Command	Description
show user-account	Displays the user account configuration.

Send comments to nx5000-docfeedback@cisco.com

vlan access-map

To create a new VLAN access map or to configure an existing VLAN access map, use the **vlan access-map** command. To remove a VLAN access map, use the **no** form of this command.

vlan access-map *map-name*

no vlan access-map *map-name*

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Each VLAN access map can include one **match** command and one **action** command.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send comments to nx5000-docfeedback@cisco.com

vlan filter

To apply a VLAN access map to one or more VLANs, use the **vlan filter** command. To unapply a VLAN access map, use the **no** form of this command.

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* [**vlan-list** *VLAN-list*]

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure.
vlan-list *VLAN-list*	Specifies the ID of one or more VLANs whose traffic the VLAN access map filters. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, use 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, use 20,70-100,142. **Note** When you use the **no** form of this command, the *VLAN-list* argument is optional. If you omit this argument, the switch removes the access map from all VLANs where the access map is applied.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can apply a VLAN access map to one or more VLANs.

You can apply only one VLAN access map to a VLAN.

The **no** form of this command enables you to unapply a VLAN access map from all or part of the VLAN list that you specified when you applied the access map. To unapply an access map from all VLANs where it is applied, you can omit the *VLAN-list* argument. To unapply an access map from a subset of the VLANs where it is currently applied, use the *VLAN-list* argument to specify the VLANs where the access map should be removed.

Examples

This example shows how to apply a VLAN access map named vlan-map-01 to VLANs 20 through 45:

```
switch(config)# vlan filter vlan-map-01 20-45
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.

Send comments to nx5000-docfeedback@cisco.com

vlan policy deny

To enter VLAN policy configuration mode for a user role, use the **vlan policy deny** command. To revert to the default VLAN policy for a user role, use the **no** form of this command.

vlan policy deny

no vlan policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All VLANs

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enter VLAN policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

This example shows how to revert to the default VLAN policy for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

vrf policy deny

To configure the deny access to a virtual forwarding and routing instance (VRF) policy for a user role, use the **vrf policy deny** command. To revert to the default VRF policy configuration for a user role, use the **no** form of this command.

vrf policy deny

no vrf policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enter VRF policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

This example shows how to revert to the default VRF policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

vsan policy deny

To configure the deny access to a VSAN policy for a user role, use the **vsan policy deny** command. To revert to the default VSAN policy configuration for a user role, use the **no** form of this command.

vsan policy deny

no vsan policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To permit access to the VSAN policy, use the **permit vsan** comand.

Examples

This example shows how to deny access to a VSAN policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)#
```

This example shows how to revert to the default VSAN policy configuration for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# no vsan policy deny
switch(config-role)#
```

Related Commands

Command	Description
permit vsan	Configures permit access to a VSAN policy for a user.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 7

System Management Commands

This chapter describes the system management commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

clear ntp statistics

To clear the Network Time Protocol (NTP) session, use the **clear ntp session** 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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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 level	Displays the results of the diagnostics tests.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.
interface	
permit	Configures a permit rule in an IPv4 ACL.
show configuration session	Displays the contents of the session.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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	Appropriate facility. The facilities are listed in the "System Message Logging Facilities" section on page 68. 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
4.0(0)N1(1a)	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
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

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

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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 appropriate outgoing *facility*. The facilities are listed in the System Message Logging Facilities section. 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

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.1(3)N2(1)	The **use-vrf** keyword was added.

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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N1(1)	The keyword **use-vrf** replaces the keyword **vrf**. The keyword **vrf** is retained for backwards compatibility.

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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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 ------------------------------------------------------------------------
          .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

Send comments to nx5000-docfeedback@cisco.com

```
   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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the logging configuration:

```
switch# show logging info
```

Send comments to nx5000-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display the last 42 lines of the log file:

```
switch# show logging last 42
```

Send comments to nx5000-docfeedback@cisco.com

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) Appropriate logging facility. The facilities are listed in the System Message Logging Facilities section.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

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

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

Related Commands	Command	Description
	logging level	Configures the facility logging level.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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
```

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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:

Send comments to nx5000-docfeedback@cisco.com

- **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.

Send comments to nx5000-docfeedback@cisco.com

  - **-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
Sun Nov  9 06:11:59 2008:  Boot Record
--------------------------------------------------------------------------------
Boot Time..........:  Sun Nov  9 06:11:58 2008
Slot Number........:  1
Serial Number......:  FLC12280050
Bios Version.......:    v1.2.0(06/19/08)
Firmware Version...:  4.0(1a)N1(1) [build 4.0(1a)N1(1)]
```

Table 7-1 describes the significant fields shown in the display.

Table 7-1 show logging onboard boot-uptime Command Output

Field	Description
Boot Time	Time boot occurred.
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.

Send comments to nx5000-docfeedback@cisco.com

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 7-2 describes the significant fields shown in the display.

Table 7-2 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
```

Send comments to nx5000-docfeedback@cisco.com

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

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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the logging session status:

```
switch# show logging session status
```

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	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

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.

Examples

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

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

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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#
```

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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
```

Send comments to nx5000-docfeedback@cisco.com

```
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#
```

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)N1(1)	This command was introduced.

Examples

This example shows how to display the SNMP sessions:

```
switch# show snmp sessions
```

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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
```

Send comments to nx5000-docfeedback@cisco.com

```
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.

Send comments to nx5000-docfeedback@cisco.com

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
4.2(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.

Send comments to nx5000-docfeedback@cisco.com

System Message Logging Facilities

Table 7-3 lists the facilities that you can use in system message logging configuration.

Table 7-3 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.
auth	Sets level for Authorization System.
authpriv	Sets level for Authorization (Private) system.
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.
dstats	Delta statistics syslog level.
epp	Sets level for EPP syslog messages.
ethpc	Sets level for ethpc syslog messages.
ethpm	Sets level for ethpm syslog messages.
evmc	Sets level for evmc syslog messages.
fabric_start_cfg_mgr	Fabric start cfg mgr syslog level.
fc2d	Sets level for fc2d syslog messages.
fcdomain	Sets level for fcdomain syslog messages.
fcns	Sets syslog filter level for name server.
fcpc	Sets level for fcpc syslog messages.
fcs	Sets syslog filter level for FCS.
fdmi	Sets logging level for fdmi.

Send comments to nx5000-docfeedback@cisco.com

Table 7-3 System Message Logging Facilities (continued)

Facility	Description
feature-mgr	Feature manager syslog level.
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.
kernel	Sets level for kernel.
l3vm	Sets syslog filter level for L3VM.
license	Licensing syslog level.
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.
mail	Sets level for Mail system.
monitor	Sets level for ethernet 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.
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.
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.

Send comments to nx5000-docfeedback@cisco.com

Table 7-3 System Message Logging Facilities (continued)

Facility	Description
rlir	Sets level for RLIR.
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.
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.
sysmgr	System Manager syslog level.
tcpudp	Sets syslog filter level for TCPUDP.
track	Sets level for track syslog messages.
urib	Sets syslog filter level for 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.
vsan	VSAN syslog level.
vshd	Sets logging level for vshd.
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.

Send comments to nx5000-docfeedback@cisco.com

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
4.0(0)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.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 8

Fibre Channel Commands

This chapter describes the Cisco NX-OS Fibre Channel, virtual Fibre Channel, and Fibre Channel over Ethernet (FCoE) commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

cfs distribute

To enable or disable Cisco Fabric Services (CFS) distribution on the switch, use the **cfs distribute** command. To disable this feature, use the **no** form of this command.

cfs distribute

no cfs distribute

Syntax Description

This command has no arguments or keywords.

Command Default

CFS distribution is enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

By default, CFS is in the distribute mode. In the distribute mode, fabric-wide distribution is enabled. Applications can distribute configuration data to all CFS-capable switches in the fabric where the application exists. This is the normal mode of operation.

If you disable CFS distribution by entering the **no cfs distribute** command, the following events occur:

- The CFS commands continue to operate. However, CFS and the applications using CFS on the switch are isolated from the rest of the fabric even though there is physical connectivity.
- All CFS operations are restricted to the isolated switch.
- CFS operations (for example, lock, commit, and abort) initiated at other switches do not have any effect at the isolated switch.
- CFS distribution is disabled over both Fibre Channel and IP.

Examples

This example shows how to disable CFS distribution:

```
switch(config)# no cfs distribute
```

This example shows how to reenable CFS distribution:

```
switch(config)# cfs distribute
```

Related Commands

Command	Description
show cfs status	Displays whether CFS distribution is enabled or disabled.

Send comments to nx5000-docfeedback@cisco.com

cfs ipv4 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv4 for applications that want to use this feature, use the **cfs ipv4** command. To disable this feature, use the **no** form of this command.

cfs ipv4 distribute

no cfs ipv4 distribute

Syntax Description

This command has no arguments or keywords.

Command Default

CFS distribution is enabled. CFS over IP is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Observe the following guidelines when using this command:

- If a switch is reachable over both IP and Fibre Channel, application data will be distributed over Fibre Channel.
- You can select either an IPv4 or IPv6 distribution when CFS is enabled over IP.
- Both IPv4 and IPv6 distribution cannot be enabled on the same switch.
- A switch that has IPv4 distribution enabled cannot detect a switch that IPv6 distribution enabled. The switches operate as if they are in two different fabrics even though they are connected to each other.

Examples

This example shows how to disable CFS IPv4 distribution:

```
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n)  [n]
```

This example shows how to reenable CFS IPv4 distribution:

```
switch(config)# cfs ipv4 distribute
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cfs ipv4 mcast-address	Configures an IPv4 multicast address for Cisco Fabric Services (CFS) distribution over IPv4.
show cfs status	Displays whether CFS distribution is enabled or disabled.

Send comments to nx5000-docfeedback@cisco.com

cfs ipv4 mcast-address

To configure an IPv4 multicast address for Cisco Fabric Services (CFS) distribution over IPv4, use the **cfs ipv4 mcast-address** command. To disable this feature, use the **no** form of this command.

cfs ipv4 mcast-address *ipv4-address*

no cfs ipv4 mcast-address *ipv4-address*

Syntax Description

ipv4-address	IPv4 multicast address for CFS distribution over IPv4. The range of valid IPv4 addresses is 239.255.0.0 through 239.255.255.255 and 239.192.0.0 through 239.251.251.251.

Command Default

Multicast address: 239.255.70.83.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before using this command, enable CFS distribution over IPv4 by using the **cfs ipv4 distribute** command.

All CFS over IP-enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

CFS distributions for application data use directed unicast.

You can configure a value for a CFS over IP multicast address. The default IPv4 multicast address is 239.255.70.83.

Examples

This example shows how to configure an IP multicast address for CFS over IPv4:

```
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

This example shows how to revert to the default IPv4 multicast address for CFS distribution over IPv4:

```
switch(config)# no cfs ipv4 mcast-address 10.1.10.100
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cfs ipv4 distribute	Enables or disables Cisco Fabric Services (CFS) distribution over IPv4.
show cfs status	Displays whether CFS distribution is enabled or disabled.

Send comments to nx5000-docfeedback@cisco.com

cfs ipv6 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv6 for applications using CFS, use the **cfs ipv6 distribute** command. To disable this feature, use the **no** form of this command.

cfs ipv6 distribute

no cfs ipv6 distribute

Syntax Description

This command has no arguments or keywords.

Command Default

CFS distribution is enabled. CFS over IPv4 is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

All CFS over IP-enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Observe the following guidelines when using this command:

- If a switch is reachable over both IP and Fibre Channel, application data will be distributed over Fibre Channel.
- You can select either an IPv4 or IPv6 distribution when CFS is enabled over IP.
- Both IPv4 and IPv6 distribution cannot be enabled on the same switch.
- A switch that has IPv4 distribution enabled cannot detect a switch that IPv6 distribution enabled. The switches operate as if they are in two different fabrics even though they are connected to each other.

Examples

This example shows how to disable CFS IPv6 distribution:

```
switch(config)# no cfs ipv6 distribute
This will prevent CFS from distributing over IPv6 network.
Are you sure? (y/n)  [n]
```

This example shows how to reenable CFS IPv6 distribution:

```
switch(config)# cfs ipv6 distribute
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cfs ipv6 mcast-address	Configures an IPv6 multicast address for Cisco Fabric Services (CFS) distribution over IPv6.
show cfs status	Displays whether CFS distribution is enabled or disabled.

Send comments to nx5000-docfeedback@cisco.com

cfs ipv6 mcast-address

To configure an IPv6 multicast address for Cisco Fabric Services (CFS) distribution over IPv6, use the **cfs ipv6 mcast-address** command. To disable this feature, use the **no** form of this command.

cfs ipv6 mcast-address *ipv6-address*

no cfs ipv6 mcast-address *ipv6-address*

Syntax Description

ipv6-address	IPv6 multicast address or CFS distribution over IPv6. The IPv6 Admin scope range is [ff15::/16, ff18::/16].

Command Default

Multicast address: ff15::efff:4653

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before using this command, enable CFS distribution over IPv6 by using the **cfs ipv6 distribute** command.

All CFS over IP-enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information. CFS distributions for application data use directed unicast.

You can configure a CFS over IP multicast address value for IPv6. The default IPv6 multicast address is ff15::efff:4653. Examples of the IPv6 Admin scope range are ff15::0000:0000 to ff15::ffff:ffff and ff18::0000:0000 to ff18::ffff:ffff.

Examples

This example shows how to configure an IP multicast address for CFS over IPv6:

```
switch(config)# cfs ipv6 mcast-address ff13::e244:4754
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

This example shows how to revert to the default IPv6 multicast address for CFS distribution over IPv6:

```
switch(config)# no cfs ipv6 mcast-address ff13::e244:4754
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cfs ipv6 distribute	Enables or disables Cisco Fabric Services (CFS) distribution over IPv6.
show cfs status	Displays whether CFS distribution is enabled or disabled.

Send comments to nx5000-docfeedback@cisco.com

cfs region

To create a region that restricts the scope of application distribution to the selected switches, use the **cfs region** command. To disable this feature, use the **no** form of this command.

cfs region *region-id*

no cfs region *region-id*

Syntax Description

region-id	Region identifier. The range is from 1 to 255. A total of 200 regions are supported.

Command Default

The default region identifier is 0.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

An application can only be a part of one region on a given switch. By creating the region ID and assigning it to an application, the application distribution is restricted to switches with a similar region ID.

Cisco Fabric Services (CFS) regions provide the ability to create distribution islands within the application scope. Currently, the regions are supported only for physical scope applications. In the absence of any region configuration, the application will be a part of the default region. The default region is region ID 0.

Examples

This example shows how to create a region ID:

```
switch(config)# cfs region 1
```

This example shows how to assign an application to a region:

```
switch(config)# cfs region 1
switch(config-cfs-region)# ntp
```

This example shows how to remove an application assigned to a region:

```
switch(config)# cfs region 1
switch(config-cfs-region)# no ntp
```

Related Commands

Command	Description
show cfs regions	Displays all configured applications with peers.

Send comments to nx5000-docfeedback@cisco.com

cfs staggered-merge

To enable Cisco Fabric Series (CFS) to merge the data from multiple Virtual SANs (VSANs), use the **cfs staggered-merge** command. To disable this feature, use the **no** form of this command.

cfs staggered-merge enable

no cfs staggered-merge enable

Syntax Description

enable	Enables the CFS staggered-merge option.

Command Default

Staggered merge is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable CFS staggered merge:

```
switch(config)# cfs staggered-merge enable
```

Related Commands

Command	Description
show cfs status	Displays whether staggered merge is enabled.

Send comments to nx5000-docfeedback@cisco.com

clear device-alias

To clear device alias information, use the **clear device-alias** command.

clear device-alias {**database** | **session** | **statistics**}

Syntax Description

database	Clears the device alias database.
session	Clears session information.
statistics	Clears device alias statistics.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the device alias session:

```
switch# clear device-alias session
```

Related Commands

Command	Description
show device-alias	Displays device alias database information.

Send comments to nx5000-docfeedback@cisco.com

clear fcdomain

To clear the entire list of configured hosts, use the **clear fcdomain** command.

clear fcdomain session vsan *vsan-id*

Syntax Description

session	Clears session information.
vsan *vsan-id*	Clears Fibre Channel domains for a specified VSAN ranging from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command clears only the list of configured hosts. Existing connections are not terminated.

Examples

This example shows how to clear the entire list of configured hosts for remote capture:

```
switch# clear fcdomain
```

Related Commands

Command	Description
show fcdomain	Displays the list of hosts configured for a remote capture.

Send comments to nx5000-docfeedback@cisco.com

clear fcflow stats

To clear Fibre Channel flow statistics, use the **clear fcflow stats** command.

clear fcflow stats [**aggregated**] **index** *flow-index*

Syntax Description

aggregated	(Optional) Clears the Fibre Channel flow aggregated statistics.
index	Clears the Fibre Channel flow counters for a specified flow index.
flow-index	Flow index number.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear aggregated Fibre Channel flow statistics for flow index 1:

```
switch(config)# clear fcflow stats aggregated index 1
```

Related Commands

Command	Description
show fcflow	Displays the fcflow statistics.

Send comments to nx5000-docfeedback@cisco.com

clear fcns statistics

To clear the name server statistics, use the **clear fcns statistics** command.

clear fcns statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Clears the FCS statistics for a specified VSAN ranging from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the name server statistics:

```
switch# clear fcns statistics vsan 1
```

Related Commands

Command	Description
show fcns statistics	Displays the name server statistics.

Send comments to nx5000-docfeedback@cisco.com

clear fcsm log

To clear the Fibre Channel Signal Modeling (FCSM) log, use the **clear fcsm log** command.

clear fcsm log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the FSCM log:

```
switch# clear fcsm log
```

Related Commands

Command	Description
show fcs	Displays the fabric configuration server information.

Send comments to nx5000-docfeedback@cisco.com

clear fcs statistics

To clear the fabric configuration server statistics, use the **clear fcs statistics** command.

clear fcs statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Clears the FCS statistics for a specified VSAN ranging from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the fabric configuration server statistics for VSAN 10:

```
switch# clear fcs statistics vsan 10
```

Related Commands

Command	Description
show fcs statistics	Displays the fabric configuration server statistics information.

Send comments to nx5000-docfeedback@cisco.com

clear fctimer session

To clear fctimer Cisco Fabric Services (CFS) session configuration and locks, use the **clear fctimer session** command.

clear fctimer session

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear an fctimer session:

```
switch# clear fctimer session
```

Related Commands

Command	Description
show fctimer	Displays fctimer information.

Send comments to nx5000-docfeedback@cisco.com

clear fspf counters

To clear the Fabric Shortest Path First (FSPF) statistics, use the **clear fspf counters** command.

clear fspf counters vsan *vsan-id* [**interface** *type*]

Syntax Description

vsan	Indicates that the counters are to be cleared for a VSAN.
vsan-id	VSAN ID. The range is from 1 to 4093.
interface *type*	(Optional) Specifies that the counters are to be cleared for an interface. The interface types are fc (Fibre Channel) and san-port-channel (SAN port channel).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If the interface is not specified, then all of the counters of a VSAN are cleared. If the interface is specified, then the counters of the specific interface are cleared.

Examples

This example shows how to clear the FSPF statistics on VSAN 1:

```
switch# clear fspf counters vsan 1
```

This example shows how to clear the FSPF statistics in VSAN 1 for the specified Fibre Channel interface:

```
switch# clear fspf counters vsan 1 interface fc 3/2
```

Related Commands

Command	Description
show fspf	Displays global FSPF information for a specific VSAN.

Send comments to nx5000-docfeedback@cisco.com

clear fc-port-security

To clear the port security information on the switch, use the **clear fc-port-security** command.

clear fc-port-security {**database auto-learn** {**interface fc** *slot*/*port* | **san-port-channel** *port*} | **session** | **statistics**} **vsan** *vsan-id*

Syntax Description

database	Clears the port security active configuration database.
auto-learn	Clears the automatically learned entries for a specified interface or VSAN.
interface fc *slot*/*port*	Clears entries for the specified Fibre Channel interface.
san-port-channel *port*	Clears entries for a specified SAN port channel. The range is from 1 to 128.
session	Clears the port security CFS configuration session and locks.
statistics	Clears the port security counters.
vsan *vsan-id*	Clears entries for a specified VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **clear fc-port-security** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **clear port-security** command.

Usage Guidelines

The active database is read-only and the **clear fc-port-security database** command can be used when resolving conflicts.

Examples

This example shows how to clear all existing statistics from the port security database for a specified VSAN:

```
switch# clear fc-port-security statistics vsan 1
```

This example shows how to clear the learned entries in the active database for a specified interface within a VSAN:

```
switch# clear fc-port-security database auto-learn interface fc2/1 vsan 1
```

This example shows how to clear the learned entries in the active database up to for the entire VSAN:

```
switch# clear fc-port-security database auto-learn vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show fc-port-security	Displays the configured port security information.

Send comments to nx5000-docfeedback@cisco.com

clear rlir

To clear Registered Link Incident Report (RLIR) information, use the **clear rlir** command.

clear rlir {**history** | **recent** {**interface fc** *slot*/*port* | **portnumber** *port*} | **statistics vsan** *vsan-id*}

Syntax Description

history	Clears RLIR incident link history.
recent	Clears recent link incidents.
interface fc *slot*/*port*	Clears entries for the specified interface.
portnumber *port*	Displays the port number for the link incidents.
statistics	Clears the RLIR statistics.
vsan *vsan-id*	Clears the RLIR statistics for a Virtual SAN (VSAN). The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the RLIR statistics for VSAN 1:

```
switch# clear rlir statistics vsan 1
```

Related Commands

Command	Description
show rlir	Displays RLIR information.

Send comments to nx5000-docfeedback@cisco.com

clear rscn session

To clear a Registered State Change Notification (RSCN) session for a specified Virtual SAN (VSAN), use the **clear rscn session** command.

clear rscn session vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN where the RSCN session should be cleared. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear an RSCN session on VSAN 1:

```
switch# clear rscn session vsan 1
```

Related Commands

Command	Description
rscn	Configures an RSCN.
show rscn	Displays RSCN information.

Send comments to nx5000-docfeedback@cisco.com

clear rscn statistics

To clear the registered state change notification statistics for a specified Virtual SAN (VSAN), use the **clear rscn statistics** command.

clear rscn statistics vsan *vsan-id*

Syntax Description

vsan	Clears the RSCN statistics for a VSAN.
vsan-id	ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to clear the RSCN statistics for VSAN 1:

```
switch# clear rscn statistics vsan 1
```

Related Commands

Command	Description
show rscn	Displays RSCN information.

Send comments to nx5000-docfeedback@cisco.com

clear zone

To clear all configured information in the zone server for a specified Virtual SAN (VSAN), use the **clear zone** command.

clear zone {**database** | **lock** | **statistics**} **vsan** *vsan-id*

Syntax Description

database	Clears zone server database information.
lock	Clears a zone server database lock.
statistics	Clears zone server statistics.
vsan	Clears zone information for a VSAN.
vsan-id	ID of the VSAN. The range is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

After entering a **clear zone database** command, you must explicitly enter the **copy running-config startup-config** command to ensure that the running configuration is used when you next start the switch.

When you enter the **clear zone lock** command from a remote switch, only the lock on that remote switch is cleared. When you enter the **clear zone lock** command from the switch where the lock originated, all locks in the VSAN are cleared. The recommended method to clear a session lock on a switch where the lock originated is by entering the **no zone commit vsan** command.

Examples

This example shows how to clear all configured information in the zone server for VSAN 1:

```
switch# clear zone database vsan 1
```

Related Commands

Command	Description
show zone	Displays zone information for any configured interface.

Send comments to nx5000-docfeedback@cisco.com

device-alias abort

To discard a Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress, use the **device-alias abort** command.

device-alias abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to discard a device alias CFS distribution session in progress:

```
switch(config)# device-alias abort
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Enables CFS distribution for device aliases.
show device-alias	Displays device alias information.

Send comments to nx5000-docfeedback@cisco.com

device-alias commit

To apply the pending configuration pertaining to the Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **device-alias commit** command.

device-alias commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to commit pending changes to the active Dynamic Port VSAN Membership (DPVM) database:

```
switch(config)# device-alias commit
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Enables CFS distribution for device aliases.
show device-alias	Displays device alias information.

Send comments to nx5000-docfeedback@cisco.com

device-alias database

To initiate a Distributed Device Alias Services (device alias) session and configure the device alias database, use the **device-alias database** command. To deactivate the device alias database, use the **no** form of this command.

device-alias database

no device-alias database

Syntax Description

This command has no arguments or keywords.

Command Default

Deactivated

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

The **device-alias database** command starts a device alias session that locks all the databases on all the switches in this fabrics. When you exit device alias database configuration mode, the device alias session ends and the locks are released.

You can only perform all modifications in the temporary device alias database. To make the changes permanent, use the **device-alias commit** command.

Examples

This example shows how to activate a device alias session and enter device alias database configuration mode:

```
switch(config)# device-alias database
switch(config-device-alias-db)#
```

Related Commands

Command	Description
device-alias commit	Commits changes from the temporary device alias database to the active device alias database.
show device-alias	Displays device alias database information.

Send comments to nx5000-docfeedback@cisco.com

device-alias distribute

To enable Cisco Fabric Services (CFS) distribution for Distributed Device Alias Services (device alias), use the **device-alias distribute** command. To disable this feature, use the **no** form of this command.

device-alias distribute

no device-alias distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

Use the **device-alias commit** command to apply pending changes to the CFS distribution session.

Examples

This example shows how to enable distribution for device alias information:

```
switch(config)# device-alias distribute
```

Related Commands

Command	Description
device-alias commit	Commits changes to the active device alias database.
device-alias database	Configures and activates the device alias database.
show device-alias	Displays device alias information.

Send comments to nx5000-docfeedback@cisco.com

device-alias import fcalias

To import device alias database information from another Virtual SAN (VSAN), use the **device-alias import fcalias** command. To revert to the default configuration or factory defaults, use the **no** form of this command.

device-alias import fcalias vsan *vsan-id*

no device-alias import fcalias vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

You can import legacy device name configurations using this feature without losing data, if they satisfy the following restrictions:

- Each fcalias has only one member.
- The member type is supported by the device name implementation.

If any name conflict exists, the fcaliases are not imported. The device name database is completely independent from the VSAN dependent fcalias database.

When the import operation is complete, the modified global fcalias table can distribute to all other switches in the physical fabric using the **device-alias distribute** command so that new definitions are available everywhere.

Examples

This example shows how to import device alias information:

```
switch(config)# device-alias import fcalias vsan 10
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Distributes fcalias database changes to the fabric.
show device-alias	Displays device alias database information.

Send comments to nx5000-docfeedback@cisco.com

device-alias mode

To configure device alias enhanced mode, use the **device-alias mode** command. To remove device alias enhanced mode, use the **no** form of this command.

device-alias mode enhanced

no device-alias mode enhanced

Syntax Description

enhanced	Specifies enhanced mode.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to configure the device alias enhanced mode:

```
switch(config)# device-alias mode enhanced
```

Related Commands

Command	Description
device-alias database	Enters device alias database configuration mode.
show device-alias	Displays device alias database information.

Send comments to nx5000-docfeedback@cisco.com

device-alias name

To configure device names in the device alias database, use the **device-alias name** command. To remove device names from the device alias database, use the **no** form of this command.

device-alias name *device-name* **pwwn** *pwwn-id*

no device-alias name *device-name*

Syntax Description

device-name	Device name. The name can be a maximum of 64 characters.
pwwn *pwwn-id*	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Command Default

None

Command Modes

Device alias database configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to configure a device name alias entry in the device name database:

```
switch(config)# device-alias database
switch(config-device-alias-db)# device-alias name Device1 pwwn 21:00:00:20:37:6f:db:bb
```

Related Commands

Command	Description
device-alias database	Enters device alias database configuration mode.
show device-alias	Displays device alias database information.

Send comments to nx5000-docfeedback@cisco.com

device-alias rename

To configure device names in the device alias database, use the **device-alias rename** command. To remove device names from the device alias database, use the **no** form of this command.

device-alias rename *device-name1 device-name2*

no device-alias rename *device-name*

Syntax Description

device-name1	Current device name.
device-name2	New device name. The maximum length is 64 characters.

Command Default

None

Command Modes

Device alias database configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to configure a device name alias entry in the device name database:

```
switch(config)# device-alias database
switch(config-device-alias-db)# device-alias rename Device1 Device2
```

Related Commands

Command	Description
device-alias database	Enters device alias database configuration mode.
show device-alias	Displays device alias database information.

Send comments to nx5000-docfeedback@cisco.com

discover custom-list

To selectively initiate discovery for specified domain IDs in a Virtual SAN (VSAN), use the **discover custom-list** command.

discover custom-list {**add** | **delete**} **vsan** *vsan-id* **domain** *domain-id*

Syntax Description

add	Adds a targets to the customized list.
delete	Deletes a target from the customized list.
vsan *vsan-id*	Discovers SCSI targets for the specified VSAN ID. The range is from 1 to 4093.
domain *domain-id*	Discovers SCSI targets for the specified domain ID. The range is from 1 to 239.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to selectively initiate the discovery for the specified VSAN and domain ID:

```
switch# discover custom-list add vsan 1 domain 2
```

This example shows how to delete the specified VSAN and domain ID from the customized list:

```
switch# discover custom-list delete vsan 1 domain 2
```

Send comments to nx5000-docfeedback@cisco.com

discover scsi-target

To discover SCSI targets on local storage to the switch or remote storage across the fabric, use the **discover scsi-target** command.

discover scsi-target {**custom-list** | **local** | **remote** | **vsan** *vsan-id* **fcid** *fc-id*} **os** {**aix** | **all** | **hpux** | **linux** | **solaris** | **windows**} [**lun** | **target**]

Syntax Description

custom-list	Discovers SCSI targets from the customized list.
local	Discovers local SCSI targets.
remote	Discovers remote SCSI targets.
vsan *vsan-id*	Discovers SCSI targets for the specified Virtual SAN (VSAN) ID. The range is from 1 to 4093.
fcid *fc-id*	Discovers SCSI targets for the specified FCID. The format is *0xhhhhhhh*, where *h* is a hexadecimal digit.
os	Discovers the specified operating system.
aix	Discovers the AIX operating system
all	Discovers all operating systems
hpux	Discovers the HPUX operating system
linux	Discovers the Linux operating system
solaris	Discovers the Solaris operating system
windows	Discovers the Windows operating system
lun	(Optional) Discovers SCSI targets and Logical Unit Numbers (LUNs).
target	(Optional) Discovers SCSI targets.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to discover local targets assigned to all OSs:

```
switch# discover scsi-target local os all
discovery started
```

This example shows how to discover remote targets assigned to the Windows OS:

```
switch# discover scsi-target remote os windows
discovery started
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to discover SCSI targets for the specified VSAN (1) and FCID (0x9c03d6):

```
switch# discover scsi-target vsan 1 fcid 0x9c03d6 os aix
discover scsi-target vsan 1 fcid 0x9c03d6
VSAN:    1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00
  PRLI RSP: 0x01 SPARM: 0x0012...
```

This example begins discovering targets from a customized list assigned to the Linux operating system:

```
switch# discover scsi-target custom-list os linux
discovery started
```

Send comments to nx5000-docfeedback@cisco.com

fabric profile

To utilize a preset quality of service (QoS) setting, use the **fabric profile** command. To restore the default, use the **no** form of this command.

fabric profile {**reliable-multicast** | **unicast-optimized**}

no fabric profile

Syntax Description

reliable-multicast	Optimizes the QoS parameters in the fabric to ensure reliable delivery of multicast traffic.
unicast-optimized	Optimizes the QoS parameters in the fabric for unicast traffic.

Command Default

Unicast-optimized

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to set the fabric to ensure reliable delivery of multicast traffic:

```
switch(config)# fabric profile reliable-multicast
```

This example shows how to set the fabric profile to the default value:

```
switch(config)# no fabric profile
```

Related Commands

Command	Description
show fabric profile	Displays the current setting of the fabric.

Send comments to nx5000-docfeedback@cisco.com

fabric-binding activate

To activate fabric binding in a Virtual SAN (VSAN), use the **fabric-binding activate** command. To disable this feature, use the **no** form of this command.

fabric-binding activate vsan *vsan-id* [**force**]

no fabric-binding activate vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.
force	(Optional) Forces fabric binding activation.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to activate the fabric binding database for the specified VSAN:

```
switch(config)# fabric-binding activate vsan 1
```

This example shows how to deactivate the fabric binding database for the specified VSAN:

```
switch(config)# no fabric-binding activate vsan 10
```

This example shows how to forcefully activate the fabric binding database for the specified VSAN:

```
switch(config)# fabric-binding activate vsan 3 force
```

This example shows how to revert to the previously configured state or to the factory default (if no state is configured):

```
switch(config)# no fabric-binding activate vsan 1 force
```

Related Commands

Command	Description
fabric-binding database	Configures a fabric-binding database.
fabric-binding enable	Enables fabric-binding.

Send comments to nx5000-docfeedback@cisco.com

fabric-binding database copy

To copy from the active fabric binding database to the configuration fabric binding database, use the **fabric-binding database copy** command.

fabric-binding database copy vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the Virtual SAN (VSAN). The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

If the configured database is empty, this command is not accepted.

Examples

This example shows how to copy from the active database to the configuration database in VSAN 1:

```
switch# fabric-binding database copy vsan 1
```

Related Commands

Command	Description
fabric-binding diff	Provides the differences between the fabric-binding databases.

Send comments to nx5000-docfeedback@cisco.com

fabric-binding database diff

To view the differences between the active database and the configuration database in a Virtual SAN (VSAN), use the **fabric-binding database diff** command.

fabric-binding database diff {**active** | **config**} **vsan** *vsan-id*

Syntax Description

active	Provides information about the differences in the active database relating to the configuration database.
config	Provides information about information on the differences in the configuration database relating to the active database.
vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

Examples

This example shows how to display the differences between the active database and the configuration database in VSAN 1:

```
switch# fabric-binding database diff active vsan 1
```

This example shows how to display information about the differences between the configuration database and the active database:

```
switch# fabric-binding database diff config vsan 1
```

Related Commands

Command	Description
fabric-binding copy	Copies from the active to the configuration fabric binding database.

Send comments to nx5000-docfeedback@cisco.com

fabric-binding database vsan

To configure a user-specified fabric binding list in a Virtual SAN (VSAN), use the **fabric-binding database vsan** command. To disable the fabric binding, use the **no** form of this command.

fabric-binding database vsan *vsan-id*
swwn *switch-wwn* **domain** *domain-id*

fabric-binding database vsan *vsan-id*
no swwn *switch-wwn* **domain** *domain-id*

no fabric-binding database vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.
swwn *switch-wwn*	Configures the switch WWN in dotted hexadecimal format.
domain *domain-id*	Specifies the specified domain ID. The domain ID is a number from 1 to 239.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis. In a Fibre Channel VSAN, only the switch world wide name (sWWN) is required; the domain ID is optional.

A user-specified fabric binding list contains a list of switch WWNs (sWWNs) within a fabric. If an sWWN attempts to join the fabric and that sWWN is not on the list, or the sWWN is using a domain ID that differs from the one specified in the allowed list, the ISL between the switch and the fabric is automatically isolated in that VSAN and the switch is denied entry into the fabric.

Examples

This example shows how to enter the fabric binding database mode and adds the sWWN and domain ID of a switch to the configured database list:

```
switch(config)# fabric-binding database vsan 5
switch(config-fabric-binding)# swwn 21:00:05:30:23:11:11:11 domain 102
```

This example shows how to delete a fabric binding database for the specified VSAN:

```
switch(config)# no fabric-binding database vsan 10
```

This example shows how to delete the sWWN and domain ID of a switch from the configured database list:

```
switch(config)# fabric-binding database vsan 5
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101
```

Related Commands

Command	Description
fabric-binding activate	Activates fabric binding.
fabric-binding enable	Enables fabric binding.

Send comments to nx5000-docfeedback@cisco.com

fabric-binding enable

To enable fabric binding in a Virtual SAN (VSAN), use the **fabric-binding enable** command. To disable fabric binding, use the **no** form of this command.

fabric-binding enable

no fabric-binding enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis.

The fabric binding feature must be enabled in each switch in the fabric that participates in the fabric binding.

Examples

This example shows how to enable fabric binding on that switch:

```
switch(config)# fabric-binding enable
```

This example shows how to disable fabric binding on that switch:

```
switch(config)# no fabric-binding enable
```

Related Commands

Command	Description
fabric-binding activate	Activates fabric binding.
fabric-binding database	Configures a fabric-binding database.

Send comments to nx5000-docfeedback@cisco.com

fc-port-security

To configure port security features and reject intrusion attempts, use the **fc-port-security** command. To negate the command or revert to the factory defaults, use the **no** form of this command.

fc-port-security {**activate vsan** *vsan-id* [**force** | **no-auto-learn**] | **auto-learn vsan** *vsan-id* | **database vsan** *vsan-id*}

no fc-port-security {**activate vsan** *vsan-id* [**force** | **no-auto-learn**] | **auto-learn vsan** *vsan-id* | **database vsan** *vsan-id*}

Syntax Description

activate	Activates a port security database for the specified VSAN and automatically enables auto-learning.
vsan *vsan-id*	Specifies the Virtual SAN (VSAN) ID. The range is from 1 to 4093.
force	(Optional) Forces the database activation.
no-auto-learn	(Optional) Disables the auto-learning feature for the port security database.
auto-learn	Enables auto-learning for the specified VSAN.
database	Enters the port security database configuration mode for the specified VSAN.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **fc-port-security** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-security** command.

Usage Guidelines

When you activate the port security feature, the **auto-learn** option is also automatically enabled. You can choose to activate the fc-port-security feature and disable auto-learning by using the **fc-port-security activate vsan** *number* **no-auto-learn** command. In this case, you need to manually populate the port security database by individually securing each port.

If the **auto-learn** option is enabled on a VSAN, you cannot activate the database for that VSAN without the **force** option.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to activate the port security database for the specified VSAN and automatically enable auto-learning:

```
switch(config)# fc-port-security activate vsan 1
```

This example shows how to deactivate the port security database for the specified VSAN and automatically disable auto-learning:

```
switch(config)# no fc-port-security activate vsan 1
```

This example shows how to disable the auto-learning feature for the port security database in VSAN 1:

```
switch(config)# fc-port-security activate vsan 1 no-auto-learn
```

This example shows how to enable auto-learning so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database.

```
switch(config)# fc-port-security auto-learn vsan 1
```

This example shows how to disable auto-learning and stops the switch from learning about new devices accessing the switch:

```
switch(config)# no fc-port-security auto-learn vsan 1
```

This example shows how to enter the port security database mode for the specified VSAN:

```
switch(config)# fc-port-security database vsan 1
switch(config-fc-port-security)#
```

This example shows how to force the VSAN 1 port security database to activate even if there are conflicts:

```
switch(config)# fc-port-security activate vsan 1 force
```

Related Commands

Command	Description
show fc-port-security database	Displays configured port security information.

Send comments to nx5000-docfeedback@cisco.com

fc-port-security abort

To discard the port security Cisco Fabric Services (CFS) distribution session in progress, use the **fc-port-security abort** command.

fc-port-security abort vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **fc-port-security abort** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-security abort** command.

Examples

This example shows how to discard a port security CFS distribution session in progress:

```
switch(config)# fc-port-security abort vsan 33
```

Related Commands

Command	Description
fc-port-security distribute	Enables CFS distribution for port security.
show fc-port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

fc-port-security commit

To apply the pending configuration pertaining to the port security Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **fc-port-security commit** command.

fc-port-security commit vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **fc-port-security commit** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-security commit** command.

Examples

This example shows how to commit changes to the active port security configuration:

```
switch(config)# fc-port-security commit vsan 13
```

Related Commands

Command	Description
fc-port-security distribute	Enables CFS distribution for port security.
show fc-port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

fc-port-security database

To copy the port security database or to view the difference within the port security database, use the **fc-port-security database** command.

fc-port-security database {**copy** | **diff** {**active** | **config**}} **vsan** *vsan-id*

Syntax Description

copy	Copies the active database to the configuration database.
diff	Provides the difference between the active and configuration port security database.
active	Writes the active database to the configuration database.
config	Writes the configuration database to the active database.
vsan *vsan-id*	Specifies the VSAN ID. The ranges is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **fc-port-security database** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-security database** command.

Usage Guidelines

If the active database is empty, the fc-port-security database is empty. Use the **fc-port-security database diff active** command to resolve conflicts.

Examples

This example shows how to copy the active database to the configured database:

```
switch# fc-port-security database copy vsan 1
```

This example shows how to provide the differences between the active database and the configuration database:

```
switch# fc-port-security database diff active vsan 1
```

This example shows how to provide information on the differences between the configuration database and the active database:

```
switch# fc-port-security database diff config vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fc-port-security database	Copies and provides information on the differences within the port security database.
show fc-port-security database	Displays configured port security information.

Send comments to nx5000-docfeedback@cisco.com

fc-port-security distribute

To enable Cisco Fabric Services (CFS) distribution for port security, use the **fc-port-security distribute** command. To disable this feature, use the **no** form of this command.

fc-port-security distribute

no fc-port-security distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **fc-port-security distribute** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-security distribute** command.

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 by using the **fc-port-security commit** command.

Examples

This example shows how to distribute the port security configuration to the fabric:

```
switch(config)# fc-port-security distribute
```

Related Commands

Command	Description
fc-port-security commit	Commits the port security configuration changes to the active configuration.
show fc-port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

fcalias clone

To clone a Fibre Channel alias, use the **fcalias clone** command.

fcalias clone *origFcalias-Name cloneFcalias-Name* **vsan** *vsan-id*

Syntax Description

origFcalias-Name cloneFcalias-Name	Fibre Channel alias. The name can be a maximum of 64 characters.
vsan	Specifies the clone Fibre Channel alias for a Virtual SAN (VSAN).
vsan-id	VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To disable a Fibre Channel alias, use the **no** form of the **fcalias name** command.

Examples

This example shows how to clone a fcalias called origAlias to cloneAlias on VSAN 45:

```
switch(config)# fcalias clone origAlias cloneAlias vsan 45
```

Related Commands

Command	Description
show fcalias	Displays the member name information in a Fibre Channel alias (fcalias).

Send comments to nx5000-docfeedback@cisco.com

fcalias name

To configure a Fibre Channel alias, use the **fcalias name** command. To disable a Fibre Channel alias, use the **no** form of this command.

fcalias name *alias-name* **vsan** *vsan-id*

no fcalias name *alias-name* **vsan** *vsan-id*

Syntax Description

alias-name	Name of the fcalias. The name can a maximum of 64 characters.
vsan	Specifies the fcalias for a Virtual SAN (VSAN).
vsan-id	VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To include multiple members in any alias, use the FCID, fWWN, or pWWN values.

Examples

This example shows how to configure an fcalias called AliasSample on VSAN 3:

```
switch(config)# fcalias name AliasSample vsan 3
switch(config-fcalias)#
```

Related Commands

Command	Description
member (fcalias configuration mode)	Configures alias members for a specified zone.

Send comments to nx5000-docfeedback@cisco.com

fcalias rename

To rename a Fibre Channel alias (fcalias), use the **fcalias rename** command. To revert to the defaults, use the **no** form of this command.

fcalias rename *current-name new-name* **vsan** *vsan-id*

no fcalias rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Current fcalias name. The name can be a maximum of 64 characters.
new-name	New fcalias name. The name can be a maximum of 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to rename an fcalias:

```
switch(config)# fcalias rename oldalias newalias vsan 10
```

Related Commands

Command	Description
fcalias name	Configures fcalias names.
show fcalias	Displays fcalias information.

Send comments to nx5000-docfeedback@cisco.com

fcdomain

To configure the Fibre Channel domain feature, use the **fcdomain** command. To disable the Fibre Channel domain, use the **no** form of this command.

fcdomain {**allowed** *domain* **vsan** *vsan-id* | **auto-reconfigure vsan** *vsan-id* | **contiguous-allocation vsan** *vsan-id* | **domain** *id* {**preferred | static**} **vsan** *vsan-id* **| fabric-name** *name* **vsan** *vsan-id* | **fcid** {**database | persistent vsan** *vsan-id*} | **optimize fast-restart vsan** *vsan-id* | **priority** *value* **vsan** *vsan-id* | **restart** [**disruptive**] **vsan** *vsan-id* | **vsan** *vsan-id*}

no fcdomain {**allowed** *domain* **vsan** *vsan-id* | **auto-reconfigure vsan** *vsan-id* | **contiguous-allocation vsan** *vsan-id* | **domain** *id* {**preferred | static**} **vsan** *vsan-id* **| fabric-name** *name* **vsan** *vsan-id* | **fcid** {**database | persistent vsan** *vsan-id*} | **optimize fast-restart vsan** *vsan-id* | **priority** *value* **vsan** *vsan-id* | **restart** [**disruptive**] **vsan** *vsan-id* | **vsan** *vsan-id*}

Syntax Description

allowed *domain*	Configures the allowed domain ID list ranging from 1 to 239.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.
auto-reconfigure	Configures autoreconfigure.
contiguous-allocation	Configures contiguous allocation.
domain *id*	Configures the domain ID and its type. The range is from 0 to 239.
preferred	Configures the domain ID as preferred. By default, the local switch accepts the domain ID assigned by the principal switch and the assigned domain ID becomes the runtime domain ID.
static	Configures the domain ID as static. The assigned domain ID is discarded, all local interfaces are isolated, and the local switch assigns itself the configured domain ID, which becomes the runtime domain ID.
fabric-name *name*	Specifies the fabric name. The name format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
fcid	Configures Fibre Channel domain persistent FC IDs.
database	Enters persistent FC IDs mode.
persistent	Enables or disables Fibre Channel domain persistent FC IDs.
optimize fast-restart	Enables a domain manager fast restart on a specified VSAN.
priority *value*	Specifies the Fibre Channel domain priority. The range is from 1 to 254.
restart	Starts a disruptive or nondisruptive reconfiguration.
disruptive	(Optional) Forces the disruptive fabric reconfiguration.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Send comments to nx5000-docfeedback@cisco.com

Usage Guidelines

You can use this command to select the principal switch, configure domain ID distribution, reconfigure the fabric, and allocate FC IDs.

We recommend using the **optimize fast-restart** option on most fabrics, especially those with a large number of logical ports (3200 or more), where a logical port is an instance of a physical port in a VSAN.

Examples

This example shows how to configure a preferred domain ID for VSAN 87:

```
switch(config)# fcdomain domain 3 preferred vsan 87
```

This example shows how to specify the disruptive fabric reconfiguration for VSAN 1:

```
switch(config)# fcdomain restart disruptive vsan 1
```

This example shows how to enable the domain manager fast restart for VSANs 7 through 10:

```
switch(config)# fcdomain optimize fast-restart vsan 7 - 10
```

This example shows how to configure the fabric world wide name (fWWN) for VSAN 3:

```
switch(config)# fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3
```

Related Commands

Command	Description
show fcdomain	Displays global information about the Fibre Channel domain configurations.

Send comments to nx5000-docfeedback@cisco.com

fcdomain abort vsan

To flush cached data without committing the cached data and release the lock, use the **fcdomain abort vsan** command. To disable the flushing of cached data, use the **no** form of this command.

fcdomain abort vsan *vsan-id*

no fcdomain abort vsan *vsan-id*

Syntax Description

vsan-id	Virtual SAN (VSAN) ID. The range is from 1 to 4093.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to flush cached data:

```
switch(config)# fcdomain abort vsan 10
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
fcdomain commit vsan	Commits cached data and releases the lock.
show fcdomain	Displays global information about the Fibre Channel domain configurations.

Send comments to nx5000-docfeedback@cisco.com

fcdomain commit vsan

To commit cached data and release the lock, use the **fcdomain commit vsan** command. To release the lock without committing the cached data, use the **no** form of this command.

fcdomain commit vsan *vsan-id*

no fcdomain commit vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to commit cached data:

```
switch(config)# fcdomain commit vsan 10
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
fcdomain abort vsan	Flushes cached data without committing and releases the lock.
show fcdomain	Displays global information about the Fibre Channel domain configurations.

Send comments to nx5000-docfeedback@cisco.com

fcdomain distribute

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

fcdomain distribute

no fcdomain distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable the fabric distribution using CFS:

```
switch(config)# fcdomain distribute
```

This example shows how to disable the fabric distribution using CFS:

```
switch(config)# no fcdomain distribute
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
show fcdomain	Displays global information about the Fibre Channel domain configurations.

Send comments to nx5000-docfeedback@cisco.com

fcdomain rcf-reject

To enable the reconfigure fabric (RCF) rejection flag for a Fibre Channel interface, use the **fcdomain rcf-reject** command. To disable this feature, use the **no** form of this command.

fcdomain rcf-reject vsan *vsan-id*

no fcdomain rcf-reject vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a Virtual SAN (VSAN) ID. The range is from 1 to 4093.

Command Default

Enabled

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this option to configure the RCF reject option for the selected Fibre Channel or virtual Fibre Channel interface.

Examples

This example shows how to configure the FCIP RCF reject fcdomain feature on a virtual Fibre Channel interface:

```
switch(config)# interface vfc 3
switch(config-if)# fcdomain rcf-reject vsan 1
```

Related Commands

Command	Description
show fcdomain	Displays global information about the Fibre Channel domain configurations.
show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

Send comments to nx5000-docfeedback@cisco.com

fcdroplatency

To configure the network and switch Fibre Channel drop latency time, use the **fcdroplatency** command. To disable the Fibre Channel latency time, use the **no** form of this command.

fcdroplatency {**network** *milliseconds* [**vsan** *vsan-id*] | **switch** *milliseconds*}

no fcdroplatency {**network** *milliseconds* [**vsan** *vsan-id*] | **switch** *milliseconds*}

Syntax Description

network *milliseconds*	Specifies network latency. The range is from 500 to 60000.
vsan *vsan-id*	(Optional) Specifies a Virtual SAN (VSAN) ID. The range is from 1 to 4093.
switch *milliseconds*	Specifies switch latency. The range is from 0 to 60000 milliseconds.

Command Default

2000 millisecond network latency

500 millisecond switch latency

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure the network latency to 5000 milliseconds:

```
switch(config)# fcdroplatency network 5000
```

This example shows how to revert to the default switch latency:

```
switch(config)# no fcdroplatency switch 4000
```

Related Commands

Command	Description
show fcdroplatency	Displays the configured Fibre Channel drop latency parameters.

Send comments to nx5000-docfeedback@cisco.com

fcflow stats

To configure fcflow statistics, use the **fcflow stats** command. To disable the counter, use the **no** form of this command.

fcflow stats {**aggregated index** *flow-number* **vsan** *vsan-id* | **index** *flow-number destination-fcid source-fcid netmask* **vsan** *vsan-id*}

no fcflow stats {**aggregated index** *flow-number* | **index** *flow-number*}

Syntax Description

aggregated	Configures aggregated fcflow statistics.
index *flow-number*	Specifies a flow index. The range is from 1 to 2147483647.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.
destination-fcid	Destination FCID in hexadecimal format.
source-fcid	Source FCID in hexadecimal format.
netmask	Mask for the source and destination FCID (restricted to 6 hexadecimal characters ranging from 0xff0000 to 0xffffff).

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you enable flow counters, you can enable a maximum of 1024 entries for aggregate flow and flow statistics. Be sure to assign an unused flow index for each new flow. The number space for the flow index is shared between the aggregate flow statistics and the flow statistics.

Examples

This example shows how to enable the aggregated flow counter:

```
switch(config)# fcflow stats aggregated index 1005 vsan 1
```

This example shows how to disable the aggregated flow counter:

```
switch(config)# no fcflow stats aggregated index 1005
```

This example shows how to enable the flow counter for a specific flow:

```
switch(config)# fcflow stats index 1 0x145601 0x5601 0xffffff vsan 1
```

This example shows how to disable the flow counter for index 1001:

```
switch(config)# no fcflow stats index 1001
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show fcflow stats	Displays the configured Fibre Channel drop latency parameters.

Send comments to nx5000-docfeedback@cisco.com

fcid-allocation

To manually add a FCID to the default area company ID list, use the **fcid-allocation** command. To remove a FCID from the default area company ID list, use the **no** form of this command.

fcid-allocation area company-id *company-id*

no fcid-allocation area company-id *company-id*

Syntax Description

area	Modifies the auto area list of company IDs.
company-id *company-id*	Configures the company IDs.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Fibre Channel standards require a unique FCID to be allocated to an N port attached to a Fx port in any switch. To conserve the number of FCIDs used, Cisco Nexus 5000 Series switches use a special allocation scheme.

Some Host Bust Adaptors (HBAs) do not discover targets that have FC IDs with the same domain and area. The switch software maintains a list of tested company IDs that do not exhibit this behavior. These HBAs were allocated with single FC IDs, and for others a full area was allocated.

To allow further scalability for switches with numerous ports, the switch software maintains a list of HBAs that exhibit this behavior. Each HBA is identified by its company ID (also known as an Organizational Unique Identifier, or OUI) used in the pWWN during a fabric login. A full area is allocated to the N ports with company IDs that are listed and for the others, a single FC ID is allocated. Regardless of the type (whole area or single) of FC ID allocated, the FC ID entries remain persistent.

Examples

This example shows how to add a new company ID to the default area company ID list:

```
switch(config)# fcid allocation area company-id 0x003223
```

Send comments to nx5000-docfeedback@cisco.com

fcinterop fcid-allocation

To allocate FCIDs on the switch, use the **fcinterop fcid-allocation** command. To disable FCIDs on the switch, use the **no** form of this command.

fcinterop fcid-allocation {**auto** | **flat** | **none**}

no fcinterop fcid-allocation {**auto** | **flat** | **none**}

Syntax Description

auto	Assigns a single FCID to compatible HBAs.
flat	Assign a single FCID.
none	Assigns an FCID range.

Command Default

The default is automatic allocation of FCIDs.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command defines how the switch assigns FCIDs.

Examples

This example shows how to set the FCID allocation to flat:

```
switch(config)# fcinterop fcid-allocation flat
```

Related Commands

Command	Description
show flogi database	Displays the fabric login (FLOGI) table.

Send comments to nx5000-docfeedback@cisco.com

fcns no-auto-poll

To enable or disable automatic polling in the name server database, use the **fcns no-auto-poll** command.

fcns no-auto-poll [**vsan** *vsan-id*] | [**wwn** *wwn-id*]

no fcns no-auto-poll [**vsan** *vsan-id*] | [**wwn** *wwn-id*]

Syntax Description

vsan *vsan-id*	(Optional) Specifies a Virtual SAN (VSAN) ID. The range is from 1 to 4093.
wwn *wwn-id*	(Optional) Specifies the port WWN, with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to disable automatic polling for VSAN 2:

```
switch(config)# fcns no-auto-poll vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

Send comments to nx5000-docfeedback@cisco.com

fcns proxy-port

To register a name server proxy, use the **fcns proxy-port** command.

fcns proxy-port *wwn-id* **vsan** *vsan-id*

no fcns proxy-port *wwn-id* **vsan** *vsan-id*

Syntax Description

wwn-id	Port WWN, with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

One name server can be configured to proxy another name server, and the name server information can be displayed using the CLI. The name server can be viewed using the CLI or the Cisco Fabric Manager.

All name server registration requests come from the same port whose parameter is registered or changed. If it does not, then the request is rejected.

Examples

This example shows how to configure a proxy port for VSAN 2:

```
switch(config)# fcns proxy-port 21:00:00:e0:8b:00:26:d vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

Send comments to nx5000-docfeedback@cisco.com

fcns reject-duplicate-pwwn vsan

To reject duplicate Fibre Channel name server (FCNS) proxies on a Virtual SAN (VSAN), use the **fcns reject-duplicate-pwwn vsan** command.

fcns reject-duplicate-pwwn vsan *vsan-id*

no fcns reject-duplicate-pwwn vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to reject duplicate FCNS pWWNs for VSAN 2:

```
switch(config)# fcns reject-duplicate-pwwn vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

Send comments to nx5000-docfeedback@cisco.com

fcoe fcf-priority

To configure the FCoE Initialization Protocol (FIP) priority value advertised by the Fibre Channel Forwarder (FCF) to FCoE nodes (ENodes), use the **fcoe fcf-priority** command. To revert to the default FCF priority value, use the **no** form of this command.

fcoe fcf-priority *value*

no fcoe fcf-priority *value*

Syntax Description

value	FCF priority value. The range is from 0 to 255, and the default is 128.

Command Default

128

Command Modes

Global configuration mode

Interface vFC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable FCoE on the switch by using the **feature fcoe** command.

The Cisco Nexus 5000 Series switch advertises its priority. The priority is used by the converged network adapters (CNAs) in the fabric to determine the best switch to connect to.

Examples

This example shows how to configure the FCF priority on the switch:

```
switch(config)# fcoe fcf-priority 50
switch(config)#
```

Related Commands

Command	Description
fcoe fcmap	Configures the FCoE MAC address prefix (FC-Map) value.
fcoe fka-adv-period	Configures the time interval at which FIP keep alive (FKA) messages are transmitted to the MAC address of the ENode.
feature fcoe	Enables FCoE on the switch.
show fcoe	Displays the FCoE parameters, such as FC-Map, default FCF priority value, and FKA advertisement period.

Send comments to nx5000-docfeedback@cisco.com

fcoe fcmap

To configure the FCoE MAC address prefix (FC-Map) used to associate the FCoE node (ENode), use the **fcoe fcmap** command. To restore the default global FC-Map value of 0xefc00, use the **no** form of this command.

fcoe fcmap *value*

no fcoe fcmap *value*

Syntax Description

value	FC-Map value. The range is from 0xefc00 to 0xefcff, and the default is 0xefc00.

Command Default

0xefc00

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable FCoE on the switch by using the **feature fcoe** command.

You can prevent data corruption due to cross-fabric talk by configuring an FC-Map, which identifies the Fibre Channel fabric for this Cisco Nexus 5000 Series switch. When the FC-Map is configured, the switch discards the MAC addresses that are not part of the current fabric.

This command requires a license.

Examples

This example shows how to configure the FC-Map value on the switch:

```
switch(config)# fcoe fcmap 0xefc10
switch(config)#
```

Related Commands

Command	Description
fcoe fcf-priority	Configures the FCoE Initialization Protocol (FIP) priority value.
fcoe fka-adv-period	Configures the time interval at which FIP keep alive (FKA) messages are transmitted to the MAC address of the ENode.
feature fcoe	Enables FCoE on the switch.
show fcoe	Displays the FCoE parameters, such as an FC-Map, default FCF priority value, and FKA advertisement period.

Send comments to nx5000-docfeedback@cisco.com

fcoe fka-adv-period

To configure the time interval at which FIP keep alive (FKA) messages are transmitted to the MAC address of the FCoE node (ENode), use the **fcoe fka-adv-period** command. To revert to the default value of 128 seconds, use the **no** form of this command.

fcoe fka-adv-period *value*

no fcoe fka-adv-period *value*

Syntax Description

value	FKA advertisement period (in seconds). The range is from 4 to 60 seconds, and the default is 8.

Command Default

8 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, FCoE must be enabled on the switch, using the **feature fcoe** command.

Examples

This example shows how to configure the FKA advertisement period for the switch to 5 seconds:

```
switch(config)# fcoe fka-adv-period 5
switch(config)#
```

Related Commands

Command	Description
fcoe fcf-priority	Configures the FCoE Initialization Protocol (FIP) priority value.
fcoe fcmap	Configures the FCoE MAC address prefix (FC-Map) used to associate the FCoE node (ENode).
feature fcoe	Enables FCoE on the switch.
show fcoe	Displays the FCoE parameters, such as an FC-Map, default FCF priority value, and FKA advertisement period.
show fcoe database	Displays the FCoE database information.

Send comments to nx5000-docfeedback@cisco.com

fcoe vsan

To map a Virtual SAN (VSAN) to a VLAN that carries Fibre Channel over Ethernet (FCoE) traffic, use the **fcoe vsan** command. To remove the mapping, use the **no** form of this command.

fcoe [**vsan** *vsan_ID*]

no fcoe [**vsan** *vsan_ID*]

Syntax Description

vsan_ID	VSAN ID. The range is from 1 to 4094.

Command Default

None

Command Modes

Vlan configuration mode.

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you map the FCoE VLAN to the VSAN, make sure that you create a VSAN using the **vsan** command in the Vsan database configuration mode.

You should use an FCoE VLAN only for FCoE. Do not use the default VLAN, VLAN1, as an FCoE VLAN. FCoE is not supported on private VLANs.

When you map a FCoE VLAN to a VSAN, ensure that the VSAN is not mapped to any other FCoE VLAN. If you map a FCoE VLAN to a VSAN that is already mapped to another FCoE VLAN, the following error appears:

```
vlan 30:another FCOE VLAN mapping exists using the requested VSAN
```

If you do not specify a VSAN number, a mapping is created from the FCoE VLAN in use to the VSAN with the same number.

Examples

This example shows how to map a FCoE VLAN to a VSAN:

```
switch(config)# vlan 30
switch(config-vlan)# fcoe vsan 337
switch(config-vlan)#
```

Related Commands

Command	Description
show vsan	Displays the configuration information of VSANs.
show vlan fcoe	Displays the FCoE VLAN to VSAN mappings.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show vsan membership	Displays VSAN membership information.
vsan	Configures the VSAN information or membership.
vsan database	Enters the VSAN database mode.

Send comments to nx5000-docfeedback@cisco.com

fcping

To ping an N port, use the **fcping** command.

fcping {**device-alias** *aliasname* | **fcid** {*fc-port* | *domain-controller-id*} | **pwwn** *pwwn-id*} **vsan** *vsan-id* [**count** *number* [**timeout** *value* [**usr-priority** *priority*]]]

Syntax Description

device-alias *aliasname*	Specifies the device alias name. The name can be a maximum of 64 characters.
fcid	Specifies the FCID of the destination N port.
fc-port	FCID port, with the format *0xhhhhhh*.
domain-controller-id	Controller ID to connect to the destination switch.
pwwn *pwwn-id*	Specifies the port WWN of the destination N port, with the format *hh:hh:hh:hh:hh:hh:hh:hh*.
vsan *vsan-id*	Specifies the VSAN ID of the destination N port. The range is from 1 to 4093.
count *number*	(Optional) Specifies the number of frames to send. A value of 0 sends forever. The range is from 0 to 2147483647.
timeout *value*	(Optional) Specifies the timeout value in seconds. The range is from 1 to 10, and the default period to wait is 5 seconds.
usr-priority *priority*	(Optional) Specifies the priority the frame receives in the switch fabric. The range is from 0 to 1.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To obtain the domain controller ID, concatenate the domain ID with FFFC. For example, if the domain ID is 0xda(218), the concatenated ID is 0xfffcda.

Examples

This example shows how to configure an fcping operation for the FCID of the destination. By default, five frames are sent.

```
switch# fcping fcid 0xd70000 vsan 1
```

This example shows how to configure the number of frames to be sent using the count option. The range is from 0 through 2147483647. A value of 0 will ping forever.

```
switch# fcping fcid 0xd70000 vsan 1 count 10
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to configure the timeout value:

```
switch# fcping fcid 0xd500b4 vsan 1 timeout 10
```

This example shows how to display the fcping operation using the device alias of the specified destination:

```
switch# fcping device-alias x vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

fcroute

To configure Fibre Channel routes and to activate policy routing, use the **fcroute** command. To remove a configuration or revert to factory defaults, use the **no** form of this command.

fcroute {*fcid* [*network-mask*] **interface** {**fc** *slot*/*port* | **san-port-channel** *port* | **vfc** *vfc-id*} **domain** *domain-id* {**metric** *number* | **remote** | **vsan** *vsan-id*}}

no fcroute {*fcid network-mask* **interface** {**fc** *slot*/*port* | **san-port-channel** *port* | **vfc** *vfc-id*} **domain** *domain-id* {**metric** *number* | **remote** | **vsan** *vsan-id*}}

Syntax Description

fcid	FC ID. The format is 0xhhhhhh.
network-mask	(Optional) Network mask of the FC ID. The format is 0x0 to 0xffffff.
interface	Specifies an interface.
fc *slot*/*port*	Specifies a Fibre Channel interface and its slot number and port number.
san-port-channel *port*	Specifies a SAN port channel interface.
vfc *vfc-id*	Specifies a virtual Fibre Channel interface.
domain *domain-id*	Specifies the route for the domain of the next hop switch. The range is from 1 to 239.
metric *number*	Specifies the cost of the route. The range is from 1 to 65535. Default cost is 10.
remote	Configures the static route for a destination switch remotely connected.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to assign forwarding information to the switch and to activate a preferred path route map.

Examples

This example shows how to specify the Fibre Channel interface and the route for the domain of the next hop switch for VSAN 2:

```
switch(config)# fcroute 0x111211 interface fc3/1 domain 3 vsan 2
```

This example shows how to specify the SAN port channel interface and the route for the domain of the next hop switch for VSAN 4:

Send comments to nx5000-docfeedback@cisco.com

```
switch(config)# fcroute 0x111211 interface san-port-channel 1 domain 3 vsan 4
```

This example shows how to specify the Fibre Channel interface, the route for the domain of the next hop switch, and the cost of the route for VSAN 1:

```
switch(config)# fcroute 0x031211 interface fc1/1 domain 3 metric 1 vsan 1
```

This example shows how to specify the Fibre Channel interface, the route for the domain of the next hop switch, the cost of the route, and configures the static route for a destination switch remotely connected for VSAN 3:

```
switch(config)# fcroute 0x111112 interface fc3/1 domain 3 metric 3 remote vsan 3
```

Related Commands

Command	Description
show fcroute	Displays Fibre Channel routes.
fcroute-map	Specifies a preferred path Fibre Channel route map.
show fcroute-map	Displays the preferred path route map configuration and status.
fcroute policy fcroute-map	Activates the preferred path Fibre Channel route map.

Send comments to nx5000-docfeedback@cisco.com

fcs plat-check-global

To enable Fabric Configuration Server (FCS) platform and node-name checking fabric wide, use the **fcs plat-check-global** command. To disable this feature, use the **no** form of this command.

fcs plat-check-global vsan *vsan-id*

no fcs plat-check-global vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID for platform checking, which is from 1 to 4096.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable FCS platform and node-name checking fabric wide:

```
switch(config)# fcs plat-check-global vsan 2
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

Send comments to nx5000-docfeedback@cisco.com

fcs register

To register Fabric Configuration Server (FCS) attributes, use the **fcs register** command. To disable this feature, use the **no** form of this command.

fcs register

no fcs register

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to register FCS attributes:

```
switch(config)# fcs register
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

Send comments to nx5000-docfeedback@cisco.com

fcs virtual-device-add

To include a virtual device in a query about zone information from an FCS, use the **fcs virtual-device-add** command. To remove a virtual device, use the **no** form of this command.

fcs virtual-device-add [**vsan-ranges** *vsan-ids*]

no fcs virtual-device-add [**vsan-ranges** *vsan-ids*]

Syntax Description

vsan-ranges *vsan-ids*	(Optional) Specifies one or multiple ranges of VSANs. The range is from 1 to 4093.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

VSAN ranges are entered as *vsan-ids*-*vsan-ids*. When you specify more than one range, separate each range with a comma. If no range is specified, the command applies to all VSANs.

Examples

This example shows how to add to one range of VSANs:

```
switch(config)# fcs virtual-device-add vsan-ranges 2-4
```

This example shows how to add to more than one range of VSANs:

```
switch(config)# fcs virtual-device-add vsan-ranges 2-4,5-8
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

Send comments to nx5000-docfeedback@cisco.com

fcsp

To configure a Fibre Channel Security Protocol (FC-SP) authentication mode for a specific interface in a FC-SP-enabled switch, use the **fcsp** command. To disable an FC-SP on the interface, use the **no** form of this command.

fcsp {**auto-active** | **auto-passive** | **on** | **off**} [*timeout-period*]

no fcsp

Syntax Description

auto-active	Configures the auto-active mode to authenticate the specified interface.
auto-passive	Configures the auto-passive mode to authenticate the specified interface.
on	Configures the on mode to authenticate the specified interface.
off	Configures the off mode to authenticate the specified interface.
timeout-period	(Optional) Time out period to reauthenticate the interface. The time ranges from 0 (default—no authentication is performed) to 100,000 minutes.

Command Default

Auto-passive mode

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To use this command, FC-SP must be enabled using the **feature fcsp** command.

Examples

This example shows how to turn on the authentication mode for Fibre Channel interface in port 1 of slot 2:

```
switch(config)# interface fc 2/1
switch(config-if)# fcsp on
switch(config-if)#
```

This example shows how to revert to the factory default of auto-passive for the selected interface:

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

This example shows how to change the selected interface to initiate FC-SP authentication but does not permit reaunthentication:

```
switch(config-if)# fcsp auto-active 0
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
feature fcsp	Enables FC-SP.
show interface	Displays an interface configuration for a specified interface.

Send comments to nx5000-docfeedback@cisco.com

fcsp dhchap

To configure DHCHAP options in a switch, use the **fcsp dhchap** command. To revert to the factory defaults, use the **no** form of this command.

fcsp dhchap {**devicename** *switch-wwn* **password** [**0** | **7**] *password* |
dhgroup [**0**] [**1**][**2**][**3**][**4**] | **hash** [**md5** | **sha1**] | **password** [**0** | **7**] *password* [**wwn** *wwn-id*]}

no fcsp dhchap {**devicename** *switch-wwn* **password** [**0** | **7**] *password* |
dhgroup [**0** | **1**| **2** | **3** | **4**] | **hash** [**md5**] [**sha1**] | **password** [**0** | **7**] *password* [*wwn-id*]}

Syntax Description

devicename	Configures a password of another device in the fabric.
switch-wwn	WWN of the device being configured.
password	Configures a DHCHAP password for the local switch.
0	(Optional) Specifies a clear text password.
7	(Optional) Specifies a password in encrypted text.
dhgroup	Configures a DHCHAP Diffie-Hellman group priority list.
0	(Optional) Specifies Null DH—no exchange is performed (default).
1 | **2** | **3** | **4**	(Optional) Specifies one or more of the groups specified by the standards.
hash	Configures a DHCHAP hash algorithm priority list in order of preference.
md5	(Optional) Specifies the MD5 hash algorithm.
sha1	(Optional) Specifies the SHA-1 hash algorithm.
wwn *wwn-id*	(Optional) Specifies the WWN ID with the format hh:hh:hh:hh:hh:hh:hh:hh.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can only see the **fcsp dhchap** command if you enter the **feature fcsp** command.

Using SHA-1 as the hash algorithm may prevent RADIUS or TACACS+ usage.

If you change the DH group configuration, make sure that you change it globally for all switches in the fabric.

Examples

This example shows how to enable FC-SP:

```
switch(config)# # feature fcsp
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to configure the use of only the SHA-1 hash algorithm:

```
switch(config)# fcsp dhchap hash sha1
```

This example shows how to configure the use of only the MD-5 hash algorithm:

```
switch(config)# fcsp dhchap hash md5
```

This example shows how to define the use of the default hash algorithm priority list of MD-5 followed by SHA-1 for DHCHAP authentication:

```
switch(config)# fcsp dhchap hash md5 sha1
```

This example shows how to revert to the factory default priority list of the MD-5 hash algorithm followed by the SHA-1 hash algorithm:

```
switch(config)# no fcsp dhchap hash sha1
```

This example shows how to prioritize the use of DH group 2, 3, and 4 in the configured order:

```
switch(config)# fcsp dhchap dhgroup 2 3 4
```

This example shows how to configure a clear text password for the local switch:

```
switch(config)# fcsp dhchap password 0 mypassword
```

This example shows how to configure a clear text password for the local switch to be used for the device with the specified WWN:

```
switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

This example shows how to configure a password entered in an encrypted format for the local switch:

```
switch(config)# fcsp dhchap password 7 sfsfdf
```

Related Commands

Command	Description
feature fcsp	Enables FC-SP.
show fcsp	Displays configured FC-SP information.

Send comments to nx5000-docfeedback@cisco.com

fcsp reauthenticate

To reauthenticate a Fibre Channel or virtual Fibre Channel interface, use the **fcsp reauthenticate** command. To revert to the factory defaults, use the **no** form of this command.

fcsp reauthenticate interface {**fc** *slot*/*port* | **vfc** *vfc-id*}

no fcsp reauthenticate interface {**fc** *slot*/*port* | **vfc** *vfc-id*}

Syntax Description

interface	Specifies the interface on which to perform the reauthentication.
interface fc *slot*/*port*	Specifies the Fibre Channel interface by the slot number and port number.
vfc *vfc-id*	Specifies the virtual Fibre Channel interface by the virtual interface group number and virtual interface ID.

Command Default

30 seconds

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure the Fibre Channel Security Protocol (FC-SP) reauthentication on a virtual Fibre Channel interface:

```
switch# fcsp reauthenticate vfc 1
```

Related Commands

Command	Description
feature fcsp	Enables FC-SP.
show fcsp	Displays configured FC-SP information.

Send comments to nx5000-docfeedback@cisco.com

fcsp timeout

To configure the timeout value for a Fibre Channel Security Protocol (FC-SP) message, use the **fcsp timeout** command. To revert to the factory defaults, use the **no** form of this command.

fcsp timeout *timeout-period*

no fcsp timeout *timeout-period*

Syntax Description

timeout-period	Timeout period. The time range is from 20 to 100 seconds.

Command Default

30 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can only see the **fcsp timeout** command if you enable FC-SP by using the **feature fcsp** command.

Examples

This example shows how to configure the FCSP timeout value:

```
switch(config)# feature fcsp
switch(config)# fcsp timeout 60
```

Related Commands

Command	Description
feature fcsp	Enables FC-SP.
show fcsp	Displays configured FC-SP information.

Send comments to nx5000-docfeedback@cisco.com

fctimer

To change the default Fibre Channel timers, use the **fctimer** command. To revert to the default values, use the **no** form of this command.

fctimer {**d_s_tov** *milliseconds* | **e_d_tov** *milliseconds* | **r_a_tov** *milliseconds*} [**vsan** *vsan-id*]

no fctimer {**d_s_tov** *milliseconds* | **e_d_tov** *milliseconds* | **r_a_tov** *milliseconds*} [**vsan** *vsan-id*]

Syntax Description

d_s_tov *milliseconds*	Specifies the distributed services timeout value (DS_TOV). The range is from 5000 to 100000 milliseconds.
e_d_tov *milliseconds*	Specifies the error detect timeout value (ED_TOV). The range is from 1000 to 100000 milliseconds, with a default of 2000.
r_a_tov *milliseconds*	Specifies the resolution allocation timeout value (RA_TOV). The range is from 5000 to 100000 milliseconds with a default of 10000.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is from 1 to 4096.

Command Default

The Fibre Channel timers have the following default values:

- 30 seconds for DS_TOV.
- 2 seconds for ED_TOV.
- 10 seconds for RA_TOV.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. In accordance with the FC-SW2 standard, these values must be the same on each switch in the fabric.

Use the **vsan** option to configure different TOV values for specific VSANs.

Examples

This example shows how to change the default Fibre Channel timers:

```
switch(config)# fctimer e_d_tov 5000
switch(config)# fctimer r_a_tov 7000
```

Related Commands

Command	Description
show fctimer	Displays the configured Fibre Channel timer values.

Send comments to nx5000-docfeedback@cisco.com

fctimer abort

To discard a Fibre Channel timer (fctimer) Cisco Fabric Services (CFS) distribution session in progress, use the **fctimer abort** command.

fctimer abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

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

```
switch(config)# fctimer abort
```

Related Commands

Command	Description
fctimer distribute	Enables CFS distribution for the fctimer.
show fctimer	Displays fctimer information.

Send comments to nx5000-docfeedback@cisco.com

fctimer commit

To apply the pending configuration pertaining to the Fibre Channel timer (fctimer) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **fctimer commit** command.

fctimer commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Examples

This example shows how to commit changes to the active Fibre Channel timer configuration:

```
switch(config)# fctimer commit
```

Related Commands

Command	Description
fctimer distribute	Enables CFS distribution for the fctimer.
show fctimer	Displays fctimer information.

Send comments to nx5000-docfeedback@cisco.com

fctimer distribute

To enable Cisco Fabric Services (CFS) distribution for the Fibre Channel timer (fctimer), use the **fctimer distribute** command. To disable this feature, use the **no** form of this command.

fctimer distribute

no fctimer distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	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 **fctimer commit** command.

Examples

This example shows how to change the default Fibre Channel timer:

```
switch(config)# fctimer distribute
```

Related Commands

Command	Description
fctimer commit	Commits the Fibre Channel timer configuration changes to the active configuration.
show fctimer	Displays fctimer information.

Send comments to nx5000-docfeedback@cisco.com

fctrace

To trace the route to an N port, use the **fctrace** command.

fctrace {**device-alias** *aliasname* | **fcid** *fcid* | **pwwn** *pwwn-id*} **vsan** *vsan-id* **[timeout** *seconds*]

Syntax Description

device-alias *aliasname*	Specifies the device alias name. The name can be a maximum of 64 characters.
fcid *fcid*	Specifies the FCID of the destination N port, with the format **0x***hhhhhh*.
pwwn *pwwn-id*	Specifies the PWWN of the destination N port, with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.
timeout *seconds*	(Optional) Specifies the the timeout value. The range is from 1 to 10.

Command Default

By default, the period to wait before timing out is 5 seconds.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to trace a route to the specified FCID in VSAN 1:

```
switch# fctrace fcid 0x660000 vsan 1
```

This example shows how to trace a route to the specified device alias in VSAN 1:

```
switch# fctrace device-alias x vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

fdmi suppress-updates

To suppress Fabric-Device Management Interface (FDMI) updates, use the **fdmi suppress-updates** command.

fdmi suppress-updates vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

By default, FDMI updates are not suppressed.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to suppress the FDMI updates in VSAN 1:

```
switch# fdmi suppress-updates vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

feature fc-port-security

To enable port security, use the **feature fc-port-security** command. To disable port security, use the **no** form of this command.

feature fc-port-security

no feature fc-port-security

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **feature fc-port-security** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-security enable** command.

Usage Guidelines

Entering the **feature fc-port-security** command enables the other commands that are used to configure FC port security.

Examples

This example shows how to enable port security:

```
switch(config)# feature fc-port-security
```

This example shows how to disable port security:

```
switch(config)# no feature fc-port-security
```

Related Commands

Command	Description
show fc-port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

feature fcsp

To enable the Fibre Channel Security Protocol (FC-SP) in a switch, use the **feature fcsp** command. To disable FC-SP, use the **no** form of this command.

feature fcsp

no feature fcsp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **feature fcsp** command has been added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **fcsp enable** command.

Usage Guidelines

Additional FC-SP commands are available when the FC-SP feature is enabled.

Examples

This example shows how to enable FC-SP:

```
switch(config)# feature fcsp
```

Related Commands

Command	Description
show fcsp	Displays configured FC-SP information.

Send comments to nx5000-docfeedback@cisco.com

feature npiv

To enable N Port Identifier Virtualization (NPIV) for all Virtual SANs (VSANs) on a switch, use the **feature npiv** command. To disable NPIV, use the **no** form of this command.

feature npiv

no feature npiv

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.1(3)N1(1)	The **feature npiv** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.1(3)N1(1), this command was known as the **npiv enable** command.

Usage Guidelines

NPIV provides a means to assign multiple port IDs to a single N port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level.

You must globally enable NPIV for all VSANs on the switch to allow the NPIV-enabled applications to use multiple N port identifiers.

Examples

This example shows how to enable NPIV for all VSANs on the switch:

```
switch(config)# feature npiv
```

This example shows how to disable NPIV for all VSANs on the switch:

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

Related Commands

Command	Description
show interface	Displays interface configurations.

Send comments to nx5000-docfeedback@cisco.com

feature npv

To enable N Port Virtualization (NPV) mode, use the **feature npv** command. To disable this feature, use the **no** form of this command.

feature npv

no feature npv

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.1(3)N1(1)	The **feature npv** command has been added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **npv enable** command.

Usage Guidelines

When NPV mode is enabled, switch configuration related to interfaces is erased and the switch is rebooted. The switch restarts in NPV mode. Configuration and verification commands for NPV are available only when NPV is enabled on the switch. When you disable NPV mode, all related configurations are automatically erased and the switch is rebooted.

Examples

This example shows how to enable NPV mode:

```
switch(config)# feature npv
```

Related Commands

Command	Description
show npv status	Displays the NPV current status.

Send comments to nx5000-docfeedback@cisco.com

feature port-track

To enable port tracking for indirect errors, use the **feature port-track** command. To disable this feature, use the **no** form of this command.

feature port-track

no feature port-track

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.1(3)N1(1)	The **feature port-track** command has been added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **port-track enable** command.

Usage Guidelines

The software brings the linked port down when the tracked port goes down. When the tracked port recovers from the failure and comes back up again, the tracked port is also brought up automatically (unless otherwise configured).

Examples

This example shows how to enable port tracking:

```
switch(config)# feature port-track
```

This example shows how to disable port tracking:

```
switch(config)# no feature port-track
```

Related Commands

Command	Description
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface san-port-channel	Displays configuration and status information for a specified SAN port channel interface.

Send comments to nx5000-docfeedback@cisco.com

fspf config

To configure an Fabric Shortest Path First (FSPF) feature for an entire Virtual SAN (VSAN), use the **fspf config** command. To delete an FSPF configuration for the entire VSAN, use the **no** form of this command.

fspf config vsan *vsan-id*
min-ls-arrival *ls-arrival-time*
min-ls-interval *ls-interval-time*
region *region-id*
spf {hold-time *spf-holdtime* **| static}**

no min-ls-arrival
no min-ls-interval
no region
no spf {hold-time | static}

no fspf config vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.
min-ls-arrival *ls-arrival-time*	Specifies the minimum time before a new link state update for a domain will be accepted by the switch. *ls-arrival-time* is an integer that specifies time in milliseconds. The range is from 0 to 65535.
min-ls-interval *ls-interval-time*	Specifies the minimum time before a new link state update for a domain will be generated by the switch. *ls-interval-time* is an integer that specifies time in milliseconds. The range is from 0 to 65535.
region *region-id*	Specifies the autonomous region to which the switch belongs. The backbone region has region-id=0. *region-id* is an unsigned integer value ranging from 0 to 255.
spf	Specifies parameters related to the shortest path first (SPF) route computation.
hold-time *spf-holdtime*	Specifies the time between two consecutive SPF computations. If the time is small, then routing will react faster to changes but CPU usage will be more. *spf-holdtime* is an integer that specifies time in milliseconds. The range is from 0 to 65535.
static	Forces static SPF computation.

Command Default

In FSPF configuration mode, the default is dynamic SPF computation.

If configuring the *spf hold-time*, the default value for FSPF is 0.

If configuring the *min-ls-arrival*, the default value for FSPF is 1000 milliseconds.

If configuring the *min-ls-interval*, the default value for FSPF is 5000 milliseconds.

Command Modes

Global configuration mode

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **fspf config** command enters FSPF configuration mode for the specified Virtual SAN (VSAN). In FSPF configuration mode, the commands configure FSPF for this VSAN.

Examples

This example shows how to configure a static SPF computation in VSAN 1 and delete the FSPF configuration in VSAN 3:

```
switch(config)# fspf config vsan 1
switch(fspf-config)# spf static
switch(fspf-config)# exit
switch(config)# no fspf config vsan 3
switch(config)#
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
fspf enable	Enables FSPF routing protocol in the specified VSAN.
fspf cost	Configures the cost for the selected interface in the specified VSAN.
fspf hello-interval	Specifies the hello message interval to verify the health of a link in the VSAN.
fspf passive	Disables the FSPF protocol for the specified interface in the specified VSAN.
fspf retransmit	Specifies the retransmit time interval for unacknowledged link state updates in the specified VSAN.

Send comments to nx5000-docfeedback@cisco.com

fspf cost

To configure Fabric Shortest Path First (FSPF) link cost for an Fibre Channel over IP (FCIP) interface, use the **fspf cost** command. To revert to the default value, use the **no** form of this command.

fspf cost *link-cost* **vsan** *vsan-id*

no fspf cost *link-cost* **vsan** *vsan-id*

Syntax Description

link-cost	FSPF link cost in seconds. The range is from 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

1000 seconds for 1 Gigabits per second interfaces

500 seconds for 2 Gigabits per second interfaces

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is not applicable to virtual Fibre Channel interfaces.

FSPF tracks the state of links on all switches in the fabric, associates a cost with each link in its database, and then chooses the path with a minimal cost. The cost associated with an interface can be changed using the **fspf cost** command to implement the FSPF route selection.

Examples

This example shows how to configure the FSPF link cost on an FCIP interface:

```
switch(config)# interface fc 2/1
switch(config-if)# fspf cost 5000 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

Send comments to nx5000-docfeedback@cisco.com

fspf dead-interval

To set the maximum interval for which a hello message must be received before the neighbor is considered lost, use the **fspf dead-interval** command. To revert to the default value, use the **no** form of this command.

fspf dead-interval *seconds* **vsan** *vsan-id*

no fspf dead-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	FSPF dead interval in seconds. The range is from 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

80 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is not applicable to virtual Fibre Channel interfaces. This value must be the same in the ports at both ends of the ISL.

Caution An error is reported at the command prompt if the configured dead time interval is less than the hello time interval.

Examples

This example shows how to configure the maximum interval of 400 seconds for a hello message before the neighbor is considered lost:

```
switch(config)# interface fc 2/1
switch(config-if)# fspf dead-interval 4000 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

Send comments to nx5000-docfeedback@cisco.com

fspf enable

To enable Fabric Shortest Path First (FSPF) for a Virtual SAN (VSAN), use the **fspf enable** command. To disable FSPF routing protocols, use the **no** form of this command.

fspf enable vsan *vsan-id*

no fspf enable vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command configures FSPF on VSANs globally.

Examples

This example shows how to enable a FSPF in VSAN 5 and disable FSPF in VSAN 7:

```
switch(config)# fspf enable vsan 5
switch(config)# no fspf enable vsan 7
```

Related Commands

Command	Description
fspf config vsan	Configures FSPF features for a VSAN.
show fspf interface	Displays information for each selected interface.

Send comments to nx5000-docfeedback@cisco.com

fspf hello-interval

To verify the health of the link, use the **fspf hello-interval** command. To revert to the default value, use the **no** form of this command.

fspf hello-interval *seconds* **vsan** *vsan-id*

no fspf hello-interval *seconds* **vsan** *vsan-id*

Syntax Description

hello-interval *seconds*	Specifies the FSPF hello interval in seconds. The range is from 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

20 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is not applicable to virtual Fibre Channel interfaces.

This command configures FSPF for the specified Fibre Channel interface. This value must be the same in the ports at both ends of the ISL.

Examples

This example shows how to configure a hello interval of 3 seconds on VSAN 1:

```
switch(config)# interface fc 2/1
switch(config-if)# fspf hello-interval 3 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.

Send comments to nx5000-docfeedback@cisco.com

fspf passive

To disable the Fabric Shortest Path First (FSPF) protocol for selected interfaces, use the **fspf passive** command. To revert to the default state, use the **no** form of this command.

fspf passive vsan *vsan-id*

no fspf passive vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

FSPF is enabled

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is not applicable to virtual Fibre Channel interfaces.

By default, FSPF is enabled on all E ports and TE ports. FSPF can be disabled by setting the interface as passive using the **fspf passive** command. FSPF must be enabled on the ports at both ends of the ISL for the protocol to operate correctly.

Examples

This example shows how to disable the FSPF protocol for the selected interface on VSAN 1:

```
switch(config)# interface fc 2/1
switch(config-if)# fspf passive vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fc	Displays an interface configuration for a specified FCIP interface.

Send comments to nx5000-docfeedback@cisco.com

fspf retransmit-interval

To specify the time after which an unacknowledged link state update should be transmitted on the interface, use the **fspf retransmit-interval** command. To revert to the default value, use the **no** form of this command.

fspf retransmit-interval *seconds* **vsan** *vsan-id*

no spf retransmit-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	FSPF retransmit interval in seconds. The range is from 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

5 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is not applicable to virtual Fibre Channel interfaces. This value must be the same in the ports at both ends of the ISL.

Examples

This example shows how to specify a retransmit interval of 6 seconds after which an unacknowledged link state update should be transmitted on the interface for VSAN 1:

```
switch(config)# interface fc 2/1
switch(config-if)# fspf retransmit-interval 6 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fc	Displays an interface configuration for a specified FCIP interface.

Send comments to nx5000-docfeedback@cisco.com

in-order-guarantee

To enable in-order delivery, use the **in-order-guarantee** command. To disable in-order delivery, use the **no** form of this command.

in-order-guarantee [**vsan** *vsan-id*]

no in-order-guarantee [**vsan** *vsan-id*] [**,**] [-]

Syntax Description

vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is from 1 to 4093.
[**,**] [-]	(Optional) Allows you to enter multiple VSANs separated by commas, or a range of VSANs separated by a dash.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

In-order delivery of data frames guarantees frame delivery to a destination in the same order that they were sent by the originator.

Examples

This example shows how to enable in-order delivery for the entire switch:

```
switch(config) # in-order-guarantee
```

This example shows how to disable in-order delivery for the entire switch:

```
switch(config)# no in-order-guarantee
```

This example shows how to enable in-order delivery for a specific VSAN:

```
switch(config)# in-order-guarantee vsan 3452
```

This example shows how to disable in-order delivery for a specific VSAN:

```
switch(config)# no in-order-guarantee vsan 101
```

Related Commands

Command	Description
show in-order-guarantee	Displays the in-order-guarantee status.

Send comments to nx5000-docfeedback@cisco.com

interface fc

To configure a Fibre Channel interface on a Cisco Nexus 5000 Series switch, use the **interface fc** command. To revert to defaults, use the **no** form of this command.

interface fc *slot/port*
channel-group {*group-id* [**force**] | **auto**}
fcdomain rcf-reject vsan *vsan-id*
fcsp {**auto-active** | **auto-passive** | **on** | **off**} [*timeout-period*]
fspf {**cost** *link-cost* **vsan** *vsan-id* | **dead-interval** *seconds* **vsan** *vsan-id* | **hello-interval** *seconds* **vsan** *vsan-id* | **passive vsan** *vsan-id* | **retransmit-interval** *seconds* **vsan** *vsan-id*}
switchport

no interface fc *slot/port*
no channel-group {*group-id* [**force**] | **auto**}
no fcdomain rcf-reject vsan *vsan-id*
no fcsp {**auto-active** | **auto-passive** | **on** | **off**}
no fspf {**cost** *link-cost* **vsan** *vsan-id* | **dead-interval** *seconds* **vsan** *vsan-id* | **hello-interval** *seconds* **vsan** *vsan-id* | **passive vsan** *vsan-id* | **retransmit-interval** *seconds* **vsan** *vsan-id*}
switchport

Syntax Description

slot/port	Slot number and port number of the interface.
channel-group	Adds to or removes from a port channel.
group-id	Port channel group number from 1 to 128.
force	(Optional) Forcefully adds a port.
auto	Enables autocreation of port channels.
fcdomain	Enters the interface mode.
rcf-reject	Configures the rcf-reject flag.
vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.
fcsp	Configures Fibre Channel Security Protocol (FC-SP) parameters for a specific interface.
auto-active	Configures the auto-active mode to authenticate the specified interface.
auto-passive	Configures the auto-passive mode to authenticate the specified interface.
on	Configures the on mode to authenticate the specified interface.
off	Configures the off mode to authenticate the specified interface.
timeout-period	(Optional) Timeout period to reauthenticate the interface. The time ranges from 0 (default—no authentication is performed) to 100,000 minutes.
fspf	Configures the FSPF parameters.
cost *link-cost*	Configures the FSPF link cost. The range is from 1 to 65535.
dead-interval *seconds*	Configures the FSPF dead interval in seconds. The range is from 2 to 65535.
hello-interval *seconds*	Configures the FSPF hello-interval. The range is from 1 to 65535.
passive	Enables or disables FSPF on the interface.
retransmit-interval *seconds*	Configures the FSPF retransmit interface in seconds. The range is from 1 to 65535.
switchport	Configures switchport parameters.

Send comments to nx5000-docfeedback@cisco.com

Command Default Disabled

Command Modes Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines You can specify a range of interfaces by entering a command with the following example format:

```
interface fc 1/1 - 5 , fc 2/5 - 7
```

See the *Cisco Nexus 5000 Series Switch CLI Software Configuration Guide* for information on port number allocation.

Use the **no shutdown** command to enable the interface.

The **interface fc** command enters interface configuration mode, which includes five commands (each with a no form). These five commands can only be used in the interface configuration mode.

The **channel-group auto** command enables autocreation of port channels. If autocreation of port channels is enabled for an interface, you must first disable this configuration before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.

Examples This example shows how to configure ports 1 to 4 in Fibre Channel interface 3:

```
switch(config)# interface fc 3/1 - 4
```

This example shows how to enable the Fibre Channel interface in port 1 of slot 3:

```
switch(config)# interface fc 3/1
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

Send comments to nx5000-docfeedback@cisco.com

interface san-port-channel

To configure a SAN port channel interface on a Cisco Nexus 5000 Series switch, use the **interface san-port-channel** command. To revert to the defaults, use the **no** form of this command.

interface san-port-channel *port* {**description** *line* | **shutdown** [**force**] | **switchport** {**mode** {**E** | **auto**} | **speed** {**1000** | **2000** | **4000** | **auto**} | **trunk** {**allowed vsan** {*vsan-id* | **add** *vsan-id* | **all**} | **mode** {**auto** | **on** | **off**}}}}

no interface san-port-channel *port* {**no description** | **no shutdown** | **no switchport** {**no mode** | **no speed** | **no trunk** {**allowed vsan** {*vsan-id* | **add** *vsan-id* | **all**}| **mode**}}}

Syntax Description

port	Port number.
description *line*	Specifies a description for the interface.
shutdown	Specifies that the interface state be changed to administrative down.
force	(Optional) Forces the interface state to administrative down.
switchport	Enters configuration parameters for the SAN port channel.
mode	Configures receive BB_credit for the specific port mode.
E	Configures E port mode.
auto	Configures autosense mode.
speed	Configures the port speed.
1000	Configures 1000-Mbps speed.
2000	Configures 2000-Mbps speed.
4000	Configures 4000-Mbps speed.
auto	Configures autosense speed.
trunk	Configures trunking parameters on the interface.
allowed	Specifies the allowed list for interface(s).
vsan	Configures the VSAN range.
vsan-id	VSAN ID. The range is from 1 to 4093.
add	Adds the VSAN ID to the range of allowed VSAN list.
all	Adds all the VSANs to allowed VSAN list.
mode	Configures the trunking mode.
off	Disables the trunking mode.
on	Enables the trunking mode.

Command Default

Disabled

Command Modes

Global configuration mode

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **interface san-port-channel** command enters interface configuration mode, which includes six commands (each with a **no** form). These commands can only be used in the interface configuration mode.

Use the **no shutdown** command to enable the interface.

Examples

This example shows how to configure SAN port channel interface 3:

```
switch(config)# interface san-port-channel 3
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

Send comments to nx5000-docfeedback@cisco.com

interface vfc

To configure a virtual Fibre Channel interface on a Cisco Nexus 5000 Series switch, use the **interface vfc** command. To revert to defaults, use the **no** form of this command.

interface vfc *vfc-id* {**bind interface ethernet** *slot/port* | **description** *line* | **shutdown** [**force**] | **switchport mode F**}

no interface vfc *vfc-id* {**no bind interface ethernet** *slot/port* | **no description | no shutdown | no switchport mode**}

Syntax Description

vfc-id	Virtual interface ID. The range is from 1 to 8192.
bind interface ethernet	Specifies that the virtual Fibre Channel interface be bound to specified Ethernet interface.
slot/port	Ethernet interface slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
description *line*	Enters a line of text to describe the interface.
shutdown	Specifies that the interface state be changed to administrative down.
force	(Optional) Specifies that the interface state be forcefully changed to administrative down.
switchport mode F	Specifies the mode of the virtual Fibre Channel interface.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can specify a range of interfaces by entering a command with the following example format:

```
interface vfc 1 - 3 , vfc 5 - 7
```

Use the **no shutdown** command to enable the interface.

Examples

This example shows how to enter interface configuration mode for virtual Fibre Channel interface 3:

```
switch(config)# interface vfc 3
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

Send comments to nx5000-docfeedback@cisco.com

lldp

To configure the Link Layer Discovery Protocol (LLDP) global options, use the **lldp** command. To remove the LLDP settings, use the **no** form of this command.

lldp {**holdtime** *seconds* | **reinit** *seconds* | **timer** *seconds*}

no lldp {**holdtime** | **reinit** | **timer**}

Syntax Description

holdtime *seconds*	Specifies the hold time (in seconds) to set the length of time that a device should save LLDP information received before discarding it. The range is from 10 to 255, and the default is 120 seconds.
reinit *seconds*	Specifies the length of time (in seconds) to wait before performing LLDP initialization on any interface. The range is from 1 to 10 seconds, and the default is 2 seconds.
timer *seconds*	Specifies the rate (in seconds) at which LLDP packets are sent. The range is from 5 to 254 seconds, and the default is 30 seconds.

Command Default

Holdtime: 120 seconds.

Reinit: 2 seconds.

Timer: 30 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable LLDP on the switch.

The LLDP settings include the length of time before discarding LLDP information received from peers, the length of time to wait before performing LLDP initialization on any interface, and the rate at which LLDP packets are sent.

Examples

This example shows how to configure the global LLDP holdtime to 200 seconds:

```
switch(config)# lldp holdtime 200
switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
feature lldp	Enables or disables LLDP on the switch.
lldp (Interface)	Configures the LLDP feature on an interface.
show lldp	Displays LLDP configuration information.

Send comments to nx5000-docfeedback@cisco.com

lldp (interface)

To enable the reception, or transmission, of Link Layer Discovery Protocol (LLDP) packets on an interface, use the **lldp** command. To disable the reception or transmission of LLDP packets, use the **no** form of this command.

lldp {**receive** | **transmit**}

no lldp {**receive** | **transmit**}

Syntax Description

receive	Specifies that the interface receive LLDP packets.
transmit	Specifies that the interface transmit LLDP packets.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before you use this command, you must enable LLDP on the switch.

Examples

This example shows how to set an interface to transmit LLDP packets:

```
switch(config)# interface ethernet 2/1
switch(config-if)# lldp transmit
switch(config-if)#
```

Related Commands

Comand	Description
feature lldp	Enables or disables LLDP on the switch.
show interface	Displays configuration information about interfaces.

Send comments to nx5000-docfeedback@cisco.com

logging abort

To discard the logging Cisco Fabric Services (CFS) distribution session in progress, 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
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
switch(config)# logging abort
```

Related Commands

Command	Description
show logging	Displays logging information.

Send comments to nx5000-docfeedback@cisco.com

logging commit

To apply the pending configuration pertaining to the logging Cisco Fabric Services (CFS) distribution session in progress 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
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
switch(config)# logging commit
```

Related Commands

Command	Description
show logging	Displays logging information.

Send comments to nx5000-docfeedback@cisco.com

logging distribute

To enable Cisco Fabric Services (CFS) distribution for logging, use the **logging distribute** command. To disable this feature, use the **no** form of this command.

logging distribute

no logging distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	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 **logging commit** command.

Examples

This example shows how to change the distribute logging configuration changes:

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

Related Commands

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

Send comments to nx5000-docfeedback@cisco.com

member (fcalias configuration mode)

To add a member name to a Fibre Channel alias on a Virtual SAN (VSAN), use the **member** command. To remove a member name from a Fibre Channel alias, use the **no** form of this command.

member {**device-alias** *aliasname* | **domain-id** *domain-id* **port-number** *port-number* **| fcid** *fc-id* | **fwwn** *fwwn-id* | **interface fc** *slot/port* [**domain-id** *domain-id* | **swwn** *swwn-id*] | **pwwn** *pwwn-id* | **symbolic-nodename** *nodename*}

no member {**device-alias** *aliasname* | **domain-id** *domain-id* **port-number** *port-number* **| fcid** *fc-id* | **fwwn** *fwwn-id* | **interface fc** *slot/port* [**domain-id** *domain-id* | **swwn** *swwn-id*] | **pwwn** *pwwn-id* | **symbolic-nodename** *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. The name can be a maximum of 64 characters.
domain-id *domain-id*	Specifies the member domain ID. The range is from 1 to 239.
port-number *port-number*	Specifies a port number in the range of 0 to 255.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh*, where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*, where *h* is a hexadecimal digit.
interface fc *slot/port*	Specifies the member interface ID and its slot number and port number.
swwn *swwn-id*	(Optional) Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*, where *h* is a hexadecimal digit.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*, where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The maximum length is 255 characters.

Command Default

None

Command Modes

Fcalias configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to add a member to an alias called samplealias:

```
switch(config)# fcalias name samplealias
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to define a Fibre Channel interface for the member:

```
switch(config-fcalias)# member interface fc3/1
```

This example shows how to delete the specified member:

```
switch(config-fcalias)# no member interface fc3/1
```

Related Commands

Command	Description
fcalias name	Configures an alias.
show fcalias	Displays the member name information in an alias.

Send comments to nx5000-docfeedback@cisco.com

member (zone configuration mode)

To add a member name to a Fibre Channel zone, use the **member** command. To remove a member name from a zone, use the **no** form of this command.

member {**device-alias** *aliasname* | **domain-id** *domain-id* **port-number** *port* | **fcalias** *alias-name* | **fcid** *fc-id* | **fwwn** *fwwn-id* | **interface fc** *slot/port* [**domain-id** *domain-id* | **swwn** *swwn-id*] | **pwwn** *pwwn-id* [**lun** *lun-id*] | **symbolic-nodename** *nodename*}

no member {**device-alias** *aliasname* | **domain-id** *domain-id* **port-number** *port* | **fcid** *fc-id* | **fwwn** *fwwn-id* | **interface fc** *slot/port* [**domain-id** *domain-id* | **swwn** *swwn-id*] | **pwwn** *pwwn-id* [**lun** *lun-id*] | **symbolic-nodename** *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. The name can be a maximum of 64 characters.
domain-id *domain-id*	Specifies the member domain ID. The range is from 1 to 239.
port-number *port*	Specifies the member port number. The range is from is 0 to 255.
fcalias *alias-name*	Specifies a Fibre Channel alias name. The name can be a maximum of 64 characters.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh*, where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*, where *h* is a hexadecimal digit.
interface fc *slot/port*	Specifies the member interface ID and its slot number and port number.
swwn *swwn-id*	(Optional) Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*, where *h* is a hexadecimal digit.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*, where *h* is a hexadecimal digit.
lun *lun-id*	(Optional) Specifies the member Logical Unit Number (LUN) ID. The format is *0***x***hhhh*[**:***hhhh*[**:***hhhh*[**:***hhhh*]]], where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The name can be a maximum of 255 characters.

Command Default

None

Command Modes

Zone set zone configuration mode and zoneset-zone configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Create a zone set zone member only if you need to add member to a zone from the zone set prompt.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to add a member to a zone called zs1 on VSAN 1:

```
switch(config)# zone name zs1 vsan 1
switch(config-zone)# member fcid 0x111112
```

This example shows how to add a zone to a zone set called Zoneset1 on VSAN 1:

```
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)# member fcid 0x111112
```

This example shows how to assign a Fibre Channel interface member into a zone:

```
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)# member interface fc 3/1
```

This example shows how to delete the specified device from a zone:

```
switch(config-zoneset-zone)# no member interface fc 3/1
```

Related Commands

Command	Description
zoneset (configuration mode)	Specifies a name for a zone set.
zone name (zone set configuration mode)	Configures a zone in a zone set.
show zoneset	Displays zone set information.

Send comments to nx5000-docfeedback@cisco.com

member (zoneset configuration mode)

To configure zone set members, use the **member** command. To remove a zone set member, use the **no** form of this command.

member *member-name*

no member *member-name*

Syntax Description

member-name	Member name. The name can be a maximum of 64 characters.

Command Default

None

Command Modes

Zone set configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to add a member zone to a zone set:

```
switch(config)# zoneset name Zoneset1 vsan 10
switch(config-zoneset)# member ZoneA
```

Related Commands

Command	Description
show zone	Displays zone information.
zoneset name	Creates a zone set.

Send comments to nx5000-docfeedback@cisco.com

npv auto-load-balance disruptive

To enable N Port Virtualization (NPV) disruptive load balancing, use the **npv auto-load-balance disruptive** command. To disable this feature, use the **no** form of this command.

npv auto-load-balance disruptive

no npv auto-load-balance disruptive

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(2a)	This command was introduced.

Usage Guidelines

Disruptive load balancing can be configured only in NPV mode.

When disruptive load balancing is enabled, NPV redistributes the server interfaces across all available NP uplinks when a new NP uplink becomes operational. To move a server interface from one NP uplink to another NP uplink, NPV forces reinitialization of the server interface so that the server performs a new login to the core switch. This action causes traffic disruption on the attached end devices.

To avoid disruption of server traffic, enable this feature only after adding a new NP uplink, and then disable it again after the server interfaces have been redistributed.

Examples

This example shows how to enable disruptive load-balancing:

```
switch(config)# npv auto-load-balance disruptive
```

Related Commands

Command	Description
feature npv	Enables NPV mode.
show npv status	Displays the NPV current status.

Send comments to nx5000-docfeedback@cisco.com

npv traffic-map

To configure an N Port Virtualization (NPV) traffic map, use the **npv traffic-map** command. To disable this feature, use the **no** form of this command.

npv traffic-map server-interface {**fc** *slot*/*port* | **vfc** *vfc-id*} **external-interface fc** *slot*/*port*

no npv traffic-map server-interface {**fc** *slot*/*port* | **vfc** *vfc-id*} **external-interface fc** *slot*/*port*

Syntax Description

server-interface	Specifies the server interface or a range of server interfaces.
fc *slot*/*port*	Specifies the slot number and port number for a native Fibre Channel interface.
vfc *vfc-id*	Specifies a virtual Fibre Channel interface.
external-interface	Specifies the NP/TNP uplink interface or a range of NP/TNP uplink interfaces that can be selected by the server interface.

Command Default

No traffic map. The switch uses automatic uplink selection to select an NP uplink for the server interface.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(2a)	This command was introduced.

Usage Guidelines

This command is only available when the switch is operating in NPV mode.

NPV traffic maps can be configured only in NPV mode.

Examples

This example shows how to create a mapping between server interface vfc1 and NP uplink fc 3/1:

```
switch(config)# npv traffic-map server-interface vfc 1 external-interface fc 3/1
```

Related Commands

Command	Description
feature npv	Enables NPV mode.
show npv status	Displays the NPV current status.

Send comments to nx5000-docfeedback@cisco.com

port-track force-shut

To force a shutdown of a tracked port, use the **port-track force-shut** command. To reenable the port tracking, use the **no** form of this command.

port-track force-shut

no port-track force-shut

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **port-track force-shut** command to keep the linked port down, even though the tracked port comes back up. You must explicitly bring the port up when required by using the **no port-track force-shut** command.

Examples

This example shows how to force the shutdown of an interface and the interfaces that it is tracking:

```
switch(config)# interface fc 2/2
switch(config-if)# no port-track force-shut
```

Related Commands

Command	Description
feature port-track	Enables port tracking.
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface san-port-channel	Displays configuration and status information for a specified SAN port channel interface.

Send comments to nx5000-docfeedback@cisco.com

port-track interface

To enable port tracking for specific interfaces, use the **port-track interface** command. To disable this feature, use the **no** form of this command.

port-track interface {**fc** *slot*/*port* | **san-port-channel** *port*} [**vsan** *vsan-id*]

no port-track interface {**fc** *slot*/*port* | **san-port-channel** *port*} [**vsan** *vsan-id*]

Syntax Description

fc *slot*/*port*	Specifies a Fibre Channel interface.
san-port-channel *port*	Specifies a SAN port channel interface. The range is from 1 to 128.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the port that an interface is tracking goes down, the interface also goes down. When the tracked port comes back up, the linked interface also comes back up. Use the **port-track force-shut** command to keep the linked interface down.

Examples

This example shows how to enable port tracking for specific interfaces:

```
switch(config)# interface fc 2/3
switch(config-if)# port-track interface san-port-channel 2
```

Related Commands

Command	Description
feature port-track	Enables port tracking.
port-track force-shut	Forcefully shuts an interface for port tracking.
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface san-port-channel	Displays configuration and status information for a specified SAN port channel interface.

Send comments to nx5000-docfeedback@cisco.com

purge fcdomain fcid

To purge persistent FCIDs, use the **purge fcdomain fcid** command.

purge fcdomain fcid vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Indicates that FCIDs are to be purged for a VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to purge all dynamic, unused FCIDs in VSAN 4:

```
switch# purge fcdomain fcid vsan 4
```

This example shows how to purge all dynamic, unused FCIDs in VSANs 4, 5, and 6:

```
switch# purge fcdomain fcid vsan 4-6
```

Send comments to nx5000-docfeedback@cisco.com

rlir preferred-cond fcid

To specify a preferred host to receive Registered Link Incident Report (RLIR) frames, use the **rlir preferred-cond fcid** command. To remove a preferred host, use the **no** form of this command.

rlir preferred-cond fcid *fc-id* **vsan** *vsan-id*

no rlir preferred-cond fcid *fc-id* **vsan** *vsan-id*

Syntax Description

fcid *fc-id*	Specifies the FC ID. The format is **0x***hhhhhh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.

Command Default

By default, the switch sends RLIR frames to one of the hosts in the Virtual SAN (VSAN) with the register function set to “conditionally receive” if no hosts have the register function set to “always receive.”

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch sends RLIR frames to the preferred host only if it meets the following conditions:

- No host in the VSAN is registered for RLIR with the registration function set to “always receive.” If one or more hosts in the VSAN are registered as “always receive,” then RLIR sends only to these hosts and not to the configured preferred host.
- The preferred host is registered with the registration function set to “conditionally receive.” If all registered hosts have the registration function set to “conditionally receive,” then the preferred host receives the RLIR frames.

You can specify only one RLIR preferred host per VSAN.

Examples

This example shows how to specify the FCID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch(config)# rlir preferred-cond fcid 0x654321 vsan 2
```

This example shows how to remove the FCID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch(config)# no rlir preferred-cond fcid 0x654321 vsan 2
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show rlir	Displays information about RLIR, Link Incident Record Registration (LIRR), and Distribute Registered Link Incident Record (DRLIR) frames.
clear rlir	Clears the RLIRs.
debug rlir	Enables RLIR debugging.

Send comments to nx5000-docfeedback@cisco.com

rscn

To configure a registered state change notification (RSCN), which is a Fibre Channel service that informs N ports about changes in the fabric, use the **rscn** command.

rscn {**multi-pid** | **suppress domain-swrscn**} **vsan** *vsan-id*

Syntax Description

multi-pid	Sends RSCNs in multiple port ID (multi-PID) format.
suppress domain-swrscn	Suppresses transmission of domain format SW-RCSNs.
vsan *vsan-id*	Configures VSAN information or membership. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure RSCNs in multi-PID format:

```
switch(config)# rscn multi-pid vsan 1
```

Related Commands

Command	Description
show rscn src-table	Displays the state change registration table.
show rscn statistics	Displays RSCN statistics.

Send comments to nx5000-docfeedback@cisco.com

rscn abort

To cancel a Registered State Change Notification (RSCN) configuration on a Virtual SAN (VSAN), use the **rscn abort** command. To reverse the cancellation, use the **no** form of this command.

rscn abort vsan *vsan-id*

no rscn abort vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN where the RSCN configuration should be canceled. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to cancel an RSCN configuration on VSAN 1:

```
switch(config)# rscn abort vsan 1
```

Related Commands

Command	Description
rscn commit	Commits a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

Send comments to nx5000-docfeedback@cisco.com

rscn commit

To apply a pending Registered State Change Notification (RSCN) configuration, use the **rscn commit** command. To discard a pending RSCN configuration, use the **no** form of this command.

rscn commit vsan *vsan-id*

no rscn commit vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN where the RSCN configuration should be committed. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you commit the changes made to the active database, the configuration is committed to all the switches in the fabric. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

Examples

This example shows how to commit an RSCN configuration on VSAN 1:

```
switch(config)# rscn commit vsan 1
```

Related Commands

Command	Description
rscn abort	Cancels a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
clear rscn session	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

Send comments to nx5000-docfeedback@cisco.com

rscn distribute

To enable distribution of a Registered State Change Notification (RSCN) configuration, use the **rscn distribute** command. To disable the distribution, use the **no** form of this command.

rscn distribute

no rscn distribute

Syntax Description

This command has no arguments or keywords.

Command Default

RSCN timer distribution is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The RSCN timer configuration must be the same on all switches in the Virtual SAN (VSAN). Cisco Fabric Service (CFS) automatically distributes the RSCN timer configuration to all switches in a fabric. Only the RSCN timer configuration is distributed.

Examples

This example shows how to enable the distribution of an RSCN configuration:

```
switch(config)# rscn distribute
```

Related Commands

Command	Description
rscn abort	Cancels a pending RSCN configuration on a specified VSAN.
rscn commit	Applies a pending RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
clear rscn session	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

Send comments to nx5000-docfeedback@cisco.com

rscn event-tov

To configure an event timeout value for a Registered State Change Notification (RSCN) on a specified Virtual SAN (VSAN), use the **rscn event-tov** command. To cancel the event timeout value and restore the default value, use the **no** form of this command.

rscn event-tov *timeout* **vsan** *vsan-id*

no rscn event-tov *timeout* **vsan** *vsan-id*

Syntax Description

timeout	Event timeout value in milliseconds. The range is from 0 to 2000.
vsan *vsan-id*	Specifies a VSAN where the RSCN event timer should be used. The ID of the VSAN is from 1 to 4093.

Command Default

The default timeout values are 2000 milliseconds for Fibre Channel VSANs.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before changing the timeout value, you must enable RSCN configuration distribution using the **rscn distribute** command.

The RSCN timer is registered with Cisco Fabric Services (CFS) during initialization and switchover.

Examples

This example shows how to configure an RSCN event timeout value on VSAN 1:

```
switch(config)# rscn event-tov 20 vsan 1
```

Related Commands

Command	Description
rscn abort	Cancels a pending RSCN configuration on a specified VSAN.
rscn commit	Applies a pending RSCN configuration.
rscn distribute	Enables distribution of an RSCN configuration.
clear rscn session	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

Send comments to nx5000-docfeedback@cisco.com

san-port-channel persistent

To convert an autocreated SAN port channel to a persistent SAN port channel, use the **san-port-channel persistent** command.

san-port-channel *port-channel-id* **persistent**

Syntax Description

port-channel-id	Port channel ID. The range is from 1 to 128.
persistent	Converts the autocreated SAN port channel to a persistent SAN port channel

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command is not reversible. A user-created channel group cannot be converted to an autocreated channel group.When the **san-port-channel persistent** command is applied to an autocreated channel group, the channel group number does not change and the properties of the member ports change to those of a user-created channel group. The channel mode remains active.

Examples

This example shows how to change the properties of an autocreated channel group to a persistent channel group:

```
switch# san-port-channel 10 persistent
```

Related Commands

Command	Description
san-port-channel protocol	Enables the SAN port channel protocol.
show interface port-channel	Displays SAN port channel interface information.
show port-channel	Displays SAN port channel information.

Send comments to nx5000-docfeedback@cisco.com

scsi-target

To configure SCSI target discovery, use the **scsi-target** command. To remove SCSI target discovery, use the **no** form of this command.

scsi-target {**auto-poll** [**vsan** *vsan-id*] | **discovery** | **ns-poll** [**vsan** *vsan-id*] | **on-demand [vsan** *vsan-id*]}

no scsi-target {**auto-poll** [**vsan** *vsan-id*] | **discovery** | **ns-poll** [**vsan** *vsan-id*] | **on-demand** [**vsan** *vsan-id*]}

Syntax Description

auto-poll	Configures SCSI target auto-polling globally or per VSAN.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is from 1 to 4093.
discovery	Configures SCSI target discovery.
ns-poll	Configures SCSI target name-server polling globally or per VSAN.
on-demand	Configures SCSI targets on-demand globally or per VSAN.

Command Default

SCSI target discovery for each option is enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Automatic global SCSI target discovery is on by default. Discovery can also be triggered for specific VSANs using on-demand, name server polling, or auto-polling options. All options are on by default. Use the **no scsi-target discovery** command to turn off all discovery options. You can also turn off specific options by using the **no** form of this command.

Examples

This example shows how to configure a SCSI target auto-polling discovery for VSAN 1:

```
switch(config)# scsi-target auto-poll vsan 1
```

This example shows how to remove the SCSI target auto-polling discovery for VSAN 1:

```
switch(config)# no scsi-target auto-poll vsan 1
```

This example shows how to configure a SCSI target discovery:

```
switch(config)# scsi-target discovery
```

This example shows how to configure a SCSI target ns-polling discovery for VSAN 1:

```
switch(config)# scsi-target ns-poll vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to remove a SCSI target ns-polling discovery for VSAN 1:

```
switch(config)# no scsi-target ns-poll vsan 1
```

This example shows how to configure a SCSI target on-demand discovery for VSAN 1:

```
switch(config)# scsi-target on-demand vsan 1
```

This example shows how to remove a SCSI target on-demand discovery for VSAN 1:

```
switch(config)# no scsi-target on-demand vsan 1
```

Related Commands

Command	Description
discover scsi-target	Discovers SCSI targets on local storage to the switch or remote storage across the fabric.
show scsi-target	Displays information about existing SCSI target configurations.

Send comments to nx5000-docfeedback@cisco.com

shutdown lan (FCoE)

To shut down the Ethernet traffic on a Fibre Channel over Ethernet (FCoE) link, use the **shutdown lan** command. To restore Ethernet traffic, use the **no** form of this command.

shutdown lan

no shutdown lan

Syntax Description

This command has no arguments or keywords.

Command Default

Not shut down.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use this command to shut down Ethernet traffic on the interface. If the interface is part of an FCoE VLAN, the shutdown has no impact on the FCoE traffic.

Examples

This example shows how to shut down an Ethernet interface on an FCoE link:

```
switch(config)# interface ethernet 2/1
switch(config-if)# shutdown lan
switch(config-if)#
```

This example shows how to restore traffic on an interface after you have shut down, or disabled, the interface:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no shutdown lan
switch(config-if)#
```

Related Commands

Command	Description
fcoe	Configures FCoE parameters.

Send comments to nx5000-docfeedback@cisco.com

switchport

To configure a switch port parameter on a Fibre Channel or virtual Fibre Channel interface, use the **switchport** command. To discard the configuration, use the **no** form of this command.

Fibre Channel Interface:

switchport
{**fcrxbbcredit** {*credit* [**mode E** | **F**] | **default** | } |
mode {**F** | **NP** | **SD**} |
speed {**1000** | **2000** | **4000** | **8000** | **auto** [**max 2000**]} |
trunk {**allowed vsan** {[**add**] *vsan-id* | **all**} | **mode** {**auto** | **off** | **on**}}}

no switchport {**fcrxbbcredit**| **mode** | **speed** | **trunk** {**allowed vsan** [[**add**] *vsan-id* | **all**] | **mode**}}

Virtual Fibre Channel Interface:

switchport mode F

Syntax Description

fcrxbbcredit	Configures receive BB_credit for the port.
credit	Receive BB_credit. The range is from 1 to 255.
mode	Configures receive BB_credit for the specific port mode.
E	Configures receive BB_credit for E or TE port mode.
F	Configures receive BB_credit for F port mode.
default	Configures default receive BB_credits depending on the port mode and capabilities.
mode	Configures the port mode.
F	Configures F port mode.
NP	Configures N port proxy mode. NP mode is valid only when the switch is operating in NPV mode.
SD	Configures SD port mode.
speed	Configures the port speed.
1000	Configures 1000-Mbps speed.
2000	Configures 2000-Mbps speed.
4000	Configures 4000-Mbps speed.
8000	Configures 8000-Mbps speed.
auto	Configures autosense speed.
max 2000	(Optional) Configures 2 Gbps as the maximum bandwidth reserved in auto mode for 24-port and 48-port 4-Gbps switching module interfaces.
trunk	Configures trunking parameters on the interface.
allowed	Specifies the allowed list for interface(s).
vsan	Configures the VSAN range.
add	(Optional) Adds the VSAN ID to the range of allowed VSAN list
vsan-id	VSAN ID. The range is from 1 to 4093.
all	Adds all the VSANs to the allowed VSAN list.

Send comments to nx5000-docfeedback@cisco.com

mode	Configures the trunking mode.
auto	Configures automatic trunking mode.
off	Disables the trunking mode.
on	Enables the trunking mode.

Command Default

The EISL encapsulation is disabled.

The default receive data buffer size is 2112 bytes.

The port mode is auto.

The speed is auto.

The maximum auto speed is 2000.

The trunk mode is on.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can specify a range of interfaces by entering a command with the following example format:

```
interface fc 1/1 - 5 , fc 2/5 - 7
```

The port speed on an interface determines the amount of shared resources available to the ports in the port group. Port group resources are reserved even though the bandwidth is not used. For example, if an interface is configured for autosensing (**auto**), then 4 Gbps of bandwidth is reserved even though the maximum operating speed is 2 Gbps. For the same interface, if autosensing with a maximum speed of 2 Gbps (**auto max 2000**) is configured, then only 2 Gbps of bandwidth is reserved and the unused 2 Gbps is shared with the other interface in the port group.

When configuring port modes, observe the following guidelines:

- Auto port mode and E port mode cannot be configured in shared rate mode.
- Shared to dedicated ports should be configured in this order: speed, port mode, credit.
- Dedicated to shared ports should be configured in this order: credit, port mode, speed.

For a virtual Fibre Channel interface, you can set the port mode to F. The remaining switch port parameters are not configurable.

Examples

This example shows how to configure the switch port parameters for a Fibre Channel interface:

```
switch(config)# interface fc 2/3
switch(config-if)# switchport description techdocsSample
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config-if)# switchport mode E
switch(config-if)# switchport trunk mode auto
switch(config-if)# switchport trunk allowed vsan all
switch(config-if)# switchport trunk allowed vsan 3
switch(config-if)# switchport trunk allowed vsan add 2
switch(config-if)# switchport fcrxbbcredit 20
```

This example shows how to configure the mode of a virtual Fibre Channel interface:

```
switch(config)# interface vfc 2
switch(config-if)# switchport mode F
```

Related Commands

Command	Description
fcrxbbcredit extended enable	Enables extended BB_credits on the switch.
show interface	Displays an interface configuration for a specified interface.

Send comments to nx5000-docfeedback@cisco.com

switchport ignore bit-errors

To prevent the detection of bit error threshold events from disabling the interface on Fibre Channel interfaces, use the **switchport ignore bit-errors** command. To revert to the default, use the **no** form of this command.

switchport ignore bit-errors

no switchport ignore bit-errors

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The bit error rate threshold is used by the switch to detect an increased error rate before performance degradation seriously affects traffic.

Bit errors can occur for the following reasons:

- Faulty or bad cable
- Faulty or bad SFP
- SFP is specified to operate at 1 Gbps but is used at 2 Gbps
- Short haul cable is used for long haul or long haul cable is used for short haul
- Momentary sync loss
- Loose cable connection at one or both ends
- Improper SFP connection at one or both ends

A bit error rate threshold is detected when 15 error bursts occur in a 5-minute period. By default, the switch disables the interface when the threshold is reached. You can enter a **shutdown/no shutdown** command sequence to reenable the interface.

Regardless of the setting of the **switchport ignore bit-errors** command, the switch generates a syslog message when bit error threshold events are detected.

Examples

This example shows how to prevent the detection of bit error events from disabling the interface:

```
switch(config)# interface fc2/1
switch(config-if)# switchport ignore bit-errors
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to allow the detection of bit error events from disabling the interface:

```
switch(config)# interface fc2/1
switch(config-if)# no switchport ignore bit-errors
```

Related Commands

Command	Description
show interface	Displays interface information.

Send comments to nx5000-docfeedback@cisco.com

system default switchport

To configure port attributes for Fibre Channel interfaces, use the **system default switchport** command. To disable port attributes, use the **no** form of this command.

system default switchport {**shutdown | trunk mode** {**auto** | **off** | **on**}}

no system default switchport {**shutdown | trunk mode** {**auto** | **off** | **on**}}

Syntax Description

shutdown	Disables or enables switch ports by default.
trunk	Configures the trunking parameters as a default.
mode	Configures the trunking mode.
auto	Enables autosense trunking.
off	Disables trunking.
on	Enables trunking.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Attributes configured using this command are applied globally to all future switch port configurations, even if you do not individually specify them at that time.

This command changes the configuration of the following ports to administrative mode F:

- All ports that are down.
- All F ports that are up, whose operational mode is F, and whose administrative mode is not F.

This command does not affect non-F ports that are up; however, if non-F ports are down, this command changes the administrative mode of those ports.

Examples

This example shows how to configure a port shutdown:

```
switch(config)# system default switchport shutdown
```

This example shows how to configure the trunk mode:

```
switch(config)# system default switchport trunk mode auto
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays Fibre Channel port modes.

Send comments to nx5000-docfeedback@cisco.com

system default zone default-zone permit

To configure default values for a zone, use the **system default zone default-zone permit** command. To revert to the defaults, use the **no** form of this command.

system default zone default-zone permit

no system default zone default-zone permit

Syntax Description

This command has no arguments or keywords.

Command Default

No default values for zones.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command defines the default values for the default zone for all Virtual SANs (VSANs). The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zone default-zone permit vsan** command to define the operational values for the default zone.

The **system default zone default-zone permit** command should only be used with VSANs that have not yet been created; it has no effect on existing VSANs.

Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

This example shows how to set the default zone to use the default values:

```
switch(config)# system default zone default-zone permit
```

This example shows how to restore the default setting:

```
switch(config)# no system default zone default-zone permit
```

Related Commands

Command	Description
zone default-zone permit vsan	Defines whether a default zone (nodes not assigned a created zone) permits or denies access to all in the default zone.
show system default zone	Displays default values for the default zone.

Send comments to nx5000-docfeedback@cisco.com

system default zone distribute full

To configure default values for distribution to a zone set, use the **system default zone distribute full** command. To revert to the defaults, use the **no** form of this command.

system default zone distribute full

no system default zone distribute full

Syntax Description

This command has no arguments or keywords.

Command Default

Distribution to active zone sets only.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command distributes the default values for the default zone to all Virtual SANs (VSANs). The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zoneset distribute full vsan** command to distribute the operational values for the default zone.

The **system default zone distribute full** command should only be used with VSANs that have not yet been created; it has no effect on existing VSANs.

Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

This example shows how to distribute the default values to the full zone set:

```
switch(config)# system default zone distribute full
```

This example shows how to distribute the default values to the active zone set only:

```
switch(config)# no system default zone distribute full
```

Related Commands

Command	Description
zoneset distribute full vsan	Distributes the operational values for the default zone to all zone sets.
show system default zone	Displays default values for the default zone.

Send comments to nx5000-docfeedback@cisco.com

trunk protocol enable

To configure the trunking protocol for Fibre Channel interfaces, use the **trunk protocol enable** command. To disable this feature, use the **no** form of this command.

trunk protocol enable

no trunk protocol enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected, and the TE port continues to function in trunking mode, but only supports traffic in Virtual SANs (VSANs) that it negotiated previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a nontrunking ISL. Before you merge traffic, you need to disable the trunking protocol.

Examples

This example shows how to disable the trunk protocol feature:

```
switch(config)# no trunk protocol enable
```

This example shows how to enable the trunk protocol feature:

```
switch(config)# trunk protocol enable
```

Related Commands

Command	Description
show trunk protocol	Displays the trunk protocol status.

Send comments to nx5000-docfeedback@cisco.com

vsan

To create multiple fabrics sharing the same physical infrastructure, assign ports to Virtual SANs (VSANs), turn on or off interop mode, load balance either per originator exchange or by source-destination ID, and VSAN membership, use the **vsan** command. To remove a configuration, use the **no** form of this command.

vsan *vsan-id*
[**interface** {**fc** *slot/port* | **san-port-channel** *port* | **vfc** *vfc-id*} |
interop [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] |
loadbalancing {**src-dst-id** | **src-dst-ox-id**} |
name *name* [**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **suspend** [**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] |
suspend [**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}]]

no vsan *vsan-id*
[**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] |
loadbalancing {**src-dst-id** | **src-dst-ox-id**} |
name *name* [**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **suspend** [**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] |
suspend [**interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}]]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4094.
interface fc *slot/port*	(Optional) Specifies the Fibre Channel interface by slot and port number on the switch.
san-port-channel *port*	Configures the SAN port channel interface specified by the SAN port channel number.
vfc *vfc-id*	Specifies the virtual Fibre Channel interface.
interop	(Optional) Turns on interoperability mode.
mode	(Optional) Interop mode. The range is from 1 to 4.
loadbalancing	(Optional) Configures the load balancing scheme.
src-dst-id	Sets src-id/dst-id for load-balancing.
src-dst-ox-id	Sets ox-id/src-id/dst-id for load balancing (default).
name *name*	Assigns a name to the VSAN. The name can be a maximum of 32 characters.
suspend	Suspends the VSAN.

Command Default

None

Command Modes

VSAN database configuration mode

Send comments to nx5000-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The VSAN ID range is increased to 4094.

Usage Guidelines

To use this command, change to the VSAN database mode.

The interface range must be in ascending order and nonoverlapping. You can specify a range using a hyphen and several interfaces using commas:

- The interface range format for a Fibre Channel interface range is fcslot/port - port , fcslot/port , fcslot/port:

  For example, **`show int fc2/1 - 3 , fc2/4 , fc3/2`**

- The format for a SAN port channel is san-port-channel portchannel-number.subinterface-number:

  For example, **`show int san-port-channel 5.1`**

There are four interop modes:

- Interop mode 1 — Standards based interop mode that requires all other vendors in the fabric to be in interop mode.
- Interop mode 2 — Brocade native mode (Core PID 0).
- Interop mode 3 — Brocade native mode (Core PID 1).
- Interop mode 4 — McData native mode. Before you configure Interop mode 4 (or remove the configuration), you must suspend the VSAN. You should unsuspend the VSAN only after you configure a VSAN-dependent switch WWN with the McData OUI [08:00:88].

The **no** form of the **vsan** *vsan-id* **interface** command is not supported. To remove a VSAN membership of an interface (for example, interface fc1/8 from VSAN 7), you must assign the interface to another VSAN. The best practice is to assign the interface back to the default VSAN (VSAN 1).

Examples

This example shows how to create multiple fabrics sharing the same physical infrastructure and how to assign ports to VSANs:

```
switch(config)# vsan database
switch-config-vsan-db# vsan 2
switch(config-vsan-db)# vsan 2 name TechDoc
switch(config-vsan-db)# vsan 2 loadbalancing src-dst-id
switch(config-vsan-db)# vsan 2 loadbalancing src-dst-ox-id
switch(config-vsan-db)# vsan 2 suspend
switch(config-vsan-db)# no vsan 2 suspend
switch(config-vsan-db)# end
```

This example shows how to suspend a VSAN and enable Interop mode 4:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 100 suspend
switch(config-vsan-db)# vsan 100 interop 4
switch(config-vsan-db)# exit
```

This example shows how to configure a VSAN to create a FCOE-VLAN to VSAN mapping:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 377
switch(config-vsan-db)# exit
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config)# vlan 30
switch(config-vlan)# fcoe vsan 337
switch(config-vlan)#
```

This example shows how to remove interface fc2/1 from VSAN 7:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interface fc2/1
switch(config-vsan-db)#
```

Related Commands

Command	Description
show vsan	Displays the configuration information of VSANs.
show vlan fcoe	Displays the FCoE VLAN to VSAN mappings.
show vsan membership	Displays VSAN membership information.
wwn vsan	Configures a WWN for a suspended VSAN that has interop mode 4 enabled.

Send comments to nx5000-docfeedback@cisco.com

vsan database

To enter Virtual SAN (VSAN) database mode to configure VSAN information and membership, use the **vsan database** command.

vsan database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To exit from the VSAN database configuration mode, use the **exit** command.

Examples

This example shows how to enter the VSAN database configuration mode:

```
switch(config)# vsan database
switch(config-vsan-db)# exit
switch(config)#
```

Related Commands

Command	Description
show vsan	Displays the configuration information of VSANs.
show vlan fcoe	Displays the FCoE VLAN to VSAN mappings.
show vsan membership	Displays VSAN membership information.
vsan	Configures VSAN information or membership.

Send comments to nx5000-docfeedback@cisco.com

wwn secondary-mac

To allocate a secondary MAC address to a SAN node, use the **wwn secondary-mac** command.

wwn secondary-mac *wwn-id* **range** *address-range*

Syntax Description

wwn-id	Secondary MAC address with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
range *address-range*	Specifies the range for the specified WWN. The only valid value is 64.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command cannot be undone.

Changes to the worldwide names are only performed as required. They should not be changed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

For more information, see the *Cisco Nexus 5000 Series Switch CLI Software Configuration Guide*.

Examples

This example shows how to allocate a secondary range of MAC addresses:

```
switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64
```

Send comments to nx5000-docfeedback@cisco.com

wwn vsan

To configure a WWN for a suspended Virtual SAN (VSAN) that has interop mode 4 enabled, use the **wwn vsan** command. To discard the configuration, use the **no** form of this command.

wwn vsan *vsan-id* **vsan-wwn** *wwn*

no wwn vsan *vsan-id* **vsan-wwn** *wwn*

Syntax Description

vsan-id	VSAN ID. The range is from 1 to 4093.
vsan-wwn *wwn*	Specifies the WWN for the VSAN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

This command can succeed only if the following conditions are satisfied:

- The VSAN must be suspended.
- The VSAN must have interop mode 4 enabled before you can specify the switch WWN for it.
- The switch WWN must be unique throughout the entire fabric.
- The configured switch WWN must have McData OUI [08:00:88].

Examples

This example shows how to assign a WWN to a VSAN:

```
switch(config)# wwn vsan 100 vsan-wwn 20:64:08:00:88:0d:5f:81
switch(config)# vsan database
switch(config-vsan-db)# vsan 100 suspend
switch(config-vsan-db)# exit
switch(config)# wwn vsan 100 vsan-wwn 20:64:08:00:88:0d:5f:81
```

Related Commands

Command	Description
vsan database	Creates multiple fabrics sharing the same physical infrastructure, assigns ports to a VSAN, turns on or off interop mode, load balances either per originator exchange or source-destination ID, and creates VSAN membership.

Send comments to nx5000-docfeedback@cisco.com

zone clone

To clone a zone name, use the **zone clone** command.

zone clone *current-zone-name new-zone-name* **vsan** *vsan-id*

Syntax Description

current-zone-name new-zone-name	Zone attribute group name. The name can be a maximum of 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **zone name (configuration mode)** command to delete the zone name.

Examples

This example shows how to create a clone of the original zone group called origZone into the clone zone group cloneZone on VSAN 45:

```
switch(config)# zone clone origZone cloneZone vsan 45
```

Related Commands

Command	Description
show zone	Displays zone information.

Send comments to nx5000-docfeedback@cisco.com

zone commit

To commit zoning changes to a Virtual SAN (VSAN), use the **zone commit** command. To negate the command, use the **no** form of this command.

zone commit vsan *vsan-id* [**force**]

no zone commit vsan *vsan-id* [**force**]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.
force	(Optional) Forces the commit.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **zone commit** command to clear a session lock on a switch where the lock originated.

Examples

This example shows how to commit zoning changes to VSAN 200:

```
switch(config)# zone commit vsan 200
```

Related Commands

Command	Description
show zone	Displays zone information.

Send comments to nx5000-docfeedback@cisco.com

zone compact

To compact a zone database in a Virtual SAN (VSAN), use the **zone compact** command.

zone compact vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

8000 zones are supported in a Cisco Nexus 5000 Series switch.

If you attempt to merge VSANs, the merge will fail if more than 2000 zones are present in a VSAN and the neighboring VSAN cannot support more than 2000 zones.

Activation will fail if more than 2000 zones are present in the VSAN and one or more switches in the fabric cannot support more than 2000 zones.

Examples

This example shows how to compact a zone database in VSAN 1:

```
switch(oongif)# zone compact vsan 1
```

Related Commands

Command	Description
show zone	Displays zone information.
show zone analysis	Displays detailed analysis and statistical information about the zoning database.

Send comments to nx5000-docfeedback@cisco.com

zone copy

To copy the active zone set to the full zone set, use the **zone copy** command. To negate the command or revert to the factory defaults, use the **no** form of this command.

zone copy active-zoneset full-zoneset [**include-auto-zones**] **vsan** *vsan-id*

zone copy vsan *vsan-id* **active-zoneset** {**bootflash:** | **ftp:** | **full-zoneset** | **scp:** | **sftp:** | **tftp:** | **volatile:**}

no zone copy

Syntax Description

active-zoneset	Copies from the active zone set.
full-zoneset	Copies the active zone set to the full-zone set.
include-auto-zones	(Optional)
vsan *vsan-id*	Configures to copy the active zone set on a VSAN to the full zone set. The ID of the VSAN is from 1 to 4093.
bootflash:	Copies the active zone set to a location in the bootflash: directory.
ftp:	Copies the active zone set to a remote location using the File Transfer Protocol (FTP) protocol.
scp:	Copies the active zone set to a remote location using the SCP protocol.
sftp:	Copies the active zone set to a remote location using the SFTP protocol.
tftp:	Copies the active zone set to a remote location using the TFTP protocol.
volatile:	Copies the active zone set to a location in the volatile: directory.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to copy the active zone set to the full zone set:

```
switch# zone copy active-zoneset full-zoneset vsan 1
```

This example shows how to copy the active zone set in VSAN 3 to a remote location using SCP:

```
switch# zone copy vsan 3 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show zone	Displays zone information.

Send comments to nx5000-docfeedback@cisco.com

zone default-zone

To define whether a default zone (assigned to nodes not assigned to a created zone) permits or denies access to all nodes in the default zone, use the **zone default-zone** command. To negate the command or revert to the factory defaults, use the **no** form of this command.

zone default-zone permit vsan *vsan-id*

no zone default-zone permit vsan *vsan-id*

Syntax Description

permit	Permits access to all nodes in the default zone.
vsan *vsan-id*	Sets default zoning behavior for the specified Virtual SAN (VSAN). The ID of the VSAN is from 1 to 4093.

Command Default

All default zones are permitted access.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **zone default-zone permit vsan** command to define the operational values for the default zone in a VSAN. This command applies to existing VSANs; it has no effect on VSANs that have not yet been created.

Use the **system default zone default-zone permit** command to use the default values defined for the default zone for all VSANs. The default values are used when you initially create a VSAN and it becomes active.

Examples

This example shows how to permit the default zoning in VSAN 2:

```
switch(config)# zone default-zone permit vsan 2
```

Related Commands

Command	Description
system default zone default-zone permit	Configures default values for a zone.
show zone	Displays zone information.

Send comments to nx5000-docfeedback@cisco.com

zone merge-control restrict vsan

To restrict zone database merging, use the **zone merge-control restrict vsan** command. To disable this feature, use the **no** form of this command.

zone merge-control restrict vsan *vsan-id*

no zone merge-control restrict vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

If merge control is set to restricted and the two databases are not identical, the merge fails and Inter-Switch Links (ISLs) between the switches become isolated.

Examples

This example shows how to set the zone merge control for VSAN 10 to restricted:

```
switch(config)# zone merge-control restrict vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

Send comments to nx5000-docfeedback@cisco.com

zone mode enhanced

To enable enhanced zoning for a Virtual SAN (VSAN), use the **zone mode enhanced** command. To disable this feature, use the **no** form of this command.

zone mode enhanced vsan *vsan-id*

no zone mode enhanced vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Before using the **zone mode enhanced** command, verify that all switches in the fabric are capable of working in enhanced zoning mode. If one or more switches are not capable of working in enhanced zoning mode, the request to enable enhanced zoning mode is rejected.

When the **zone mode enhanced vsan** command completes successfully, the software automatically starts a session, distributes the zoning database using the enhanced zoning data structures, applies the configuration changes, and sends a release change authorization (RCA) to all switches in the fabric. All switches in the fabric then enable enhanced zoning mode.

Examples

This example shows how to enable enhanced zoning mode:

```
switch(config)# zone mode enhanced vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

Send comments to nx5000-docfeedback@cisco.com

zone name (configuration mode)

To create a zone, use the **zone name** command. To negate the command or revert to the factory defaults, use the **no** form of this command.

zone name *zone-name* **vsan** *vsan-id*
member

zone name *zone-name* **vsan** *vsan-id*
no member

no zone name *zone-name* **vsan** *vsan-id*

Syntax Description

zone-name	Name of the zone. The name can be a maximum of 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Zones are assigned to zone sets. Zone sets are then activated from one switch and propagate across the fabric to all switches. Zones allow security by permitting and denying access between nodes (hosts and storage). **zone name** commands are entered from the configuration mode. Configure a zone for a VSAN from the config-zone mode.

Use the **show wwn switch** command to retrieve the switch world wide name (sWWN). If you do not provide an sWWN, the software automatically uses the local sWWN.

Examples

This example shows how to configure attributes for the specified zone (Zone1) based on the member type (pWWN, fabric pWWN, FCID, or Fibre Channel alias) and value specified:

```
switch(config)# zone name Zone1 vsan 10
switch(config-zone)# member device-alias device1
```

This example shows how to configure the members for the specified zone (Zone2) based on the member type (pWWN, fabric pWWN, FCID, or Fibre Channel alias) and value specified:

```
switch(config)# zone name Zone2 vsan 10
switch(config-zone)# member fcalias Payroll
switch(config-zone)# member domain-id 2 portnumber 23
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show zone	Displays zone information.
zone rename	Renames zones.
zone-attribute-group name	Configures zone attribute groups.

Send comments to nx5000-docfeedback@cisco.com

zone name (zone set configuration mode)

To configure a zone in a zone set, use the **zone name** command. To delete the zone from the zone set, use the **no** form of this command.

zone name *zone-name*

no zone name *zone-name*

Syntax Description

zone-name	Name of the zone. The name can be a maximum of 64 characters.

Command Default

None

Command Modes

Zone set configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to configure a zone in a zone set:

```
switch(config)# zoneset name Sample vsan 1
switch(config-zoneset)# zone name MyZone
```

This example shows how to delete a zone from a zone set:

```
switch(config-zoneset)# no zone name Zone2
switch(config-zoneset)#
```

Related Commands

Command	Description
show zoneset	Displays zone set information.
zone name (configuration mode)	Configure zones.
zoneset	Configures zone set attributes.

Send comments to nx5000-docfeedback@cisco.com

zone rename

To rename a zone, use the **zone rename** command.

zone rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Current fcalias name. The name can be a maximum of 64 characters.
new-name	New fcalias name. The name can be a maximum of 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to rename a zone:

```
switch# zone rename ZoneA ZoneB vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.
zone name	Creates and configures zones.

Send comments to nx5000-docfeedback@cisco.com

zoneset (configuration mode)

To group zones under one zone set, use the **zoneset** command. To negate the command or revert to the factory defaults, use the **no** form of this command.

zoneset {**activate** [**name** *zoneset-name*] **vsan** *vsan-id* | **clone** *zoneset-currentName zoneset-cloneName* **vsan** *vsan-id* | **distribute full vsan** *vsan-id* **name** *zoneset-name* **vsan** *vsan-id* | **rename** *current-name new-name* **vsan** *vsan-id*}

no zoneset {**activate** [**name** *zoneset-name*] **vsan** *vsan-id* | **clone** *zoneset-currentName zoneset-cloneName* **vsan** *vsan-id* | **distribute full vsan** *vsan-id* **name** *zoneset-name* **vsan** *vsan-id* | **rename** *current-name new-name* **vsan** *vsan-id*}

Syntax Description

activate	Activates a zone set
name *zoneset-name*	(Optional) Specifies a name for a zone set. The name can be a maximum of 64 characters.
vsan *vsan-id*	Activates a zone set on the specified Virtual SAN (VSAN). The range is from 1 to 4093.
clone *zoneset-currentName zoneset-cloneName*	Clones a zone set from the current name to a new name. The name can be a maximum of 64 characters.
distribute full	Enables zone set propagation.
rename	Renames a zone set.
current-name	Current fcalias name.
new-name	New fcalias name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Zones are activated by activating the parent zone set.

The **zoneset distribute full vsan** command distributes the operational values for the default zone to all zone sets in a VSAN. If you do not want to distribute the operation values, use the **system default zone distribute full** command to distribute the default values.The default values are used when you initially create a VSAN and it becomes active.

The **zoneset distribute full vsan** command applies to existing VSANs; it has no effect on VSANs that have not yet been created.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to activate a zone set called zSet1 in VSAN 333:

```
switch(config)# zoneset activate name zSet1 vsan 333
```

This example shows how to clone a zone set called zSet1 into a new zoneset called zSetClone in VSAN 45:

```
switch(config)# zoneset clone existing zSet1 zSetClone vsan 45
```

This example shows how to distribute the operational values for the default zone to all zone sets in VSAN 22:

```
switch(config)# zoneset distribute full vsan 22
```

Related Commands

Command	Description
system default zone distribute full	Configures default values for distribution to a zone set
show zoneset	Displays zone set information.

Send comments to nx5000-docfeedback@cisco.com

zoneset (EXEC mode)

To merge zone set databases, use the **zoneset** command.

zoneset {**distribute** | **export** | **import interface** {*fc slot/port* | **san-port-channel** *port-number*}} **vsan** *vsan-id*

Syntax Description

distribute	Distributes the full zone set in the fabric.
export	Exports the zone set database to the adjacent switch on the specified Virtual SAN (VSAN). The active zone set in this switch becomes the activated zone set of the merged SAN.
import	Imports the zone set database to the adjacent switch on the specified interface. The active zone set in the adjacent switch becomes the activated zone set of the merged SAN.
interface	Configures the interface.
fc *slot/port*	Configures a Fibre Channel interface for the specified slot number and port number.
san-port-channel *port-number*	Specifies a SAN port channel interface.
vsan *vsan-id*	Merges the zone set database of a VSAN on the specified interface. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can also enter the **zoneset import** and the **zoneset export** commands for a range of VSANs.

The **zoneset distribute vsan** *vsan-id* command is supported in interop 2 and interop 3 modes, and not in interop 1 mode.

Examples

This example shows how to import the zone set database from the adjacent switch connected through the VSAN 2 interface:

```
switch# zoneset import interface fc2/3 vsan 2
```

This example shows how to export the zone set database to the adjacent switch connected through VSAN 5:

```
switch# zoneset export vsan 5
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to distribute the zone set in VSAN 333:

```
switch# zoneset distribute vsan 333
```

Related Commands

Command	Description
show zone status vsan	Displays the distribution status for the specified VSAN.
show zoneset	Displays zone set information.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 9

Fibre Channel Show Commands

This chapter describes the Cisco NX-OS Fibre Channel, virtual Fibre Channel, and Fibre Channel over Ethernet (FCoE) **show** commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

show cfs

To display Cisco Fabric Services (CFS) information, use the **show cfs** command.

show cfs {**application** [**name** *app-name*] | **lock** [**name** *app-name* [**vsan** *vsan-id*]] | **merge status** [**name** *app-name* [**vsan** *vsan-id*]] | **peers** [**name** *app-name* [**vsan** *vsan-id*]] | **regions** | **status**}

Syntax Description

application	Displays locally registered applications.
name *app-name*	(Optional) Specifies a local application information by name. The name can be a maximum of 64 characters.
lock	Displays the state of application logical or physical locks.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is from 1 to 4093.
merge status	Displays CFS merge information.
peers	Displays logical or physical CFS peers.
regions	Displays the CFS regions.
status	Displays if CFS distribution is enabled or disabled. Enabled is the default configuration.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show cfs application** command displays only those applications that are registered with CFS. Conditional services that use CFS do not appear in the output unless those services are running.

Examples

This example shows how to display the CFS physical peer information for all applications:

```
switch# show cfs peers
```

This example shows how to display the CFS information for all applications on the switch:

```
switch# show cfs application
```

This example shows how to display the status of the CFS distribution:

```
switch# show cfs status
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
cfs	Configures Cisco Fabric Services (CFS) information.

Send comments to nx5000-docfeedback@cisco.com

show debug npv

To display the N Port Virtualization (NPV) debug commands configured on the switch, use the **show debug npv** command.

show debug npv

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show debug npv** command is available only when the switch is in NPV mode.

Examples

This example shows how to display all the NPV debug commands available on the switch:

```
switch# show debug npv
```

Related Commands

Command	Description
debug npv	Enables debugging NPV configurations.

Send comments to nx5000-docfeedback@cisco.com

show device-alias

To display the device name information, use the **show device-alias** command.

show device-alias {**database** | **merge status** | **name** *device-name* [**pending**] | **pending** | **pending-diff** | **pwwn** *pwwn-id* [**pending**] | **session status** | **statistics** | **status**

Syntax Description

database	Displays the entire device name database.
merge status	Displays the device merge status.
name *device-name*	Displays device name database information for a specific device name.
pending	(Optional) Displays the pending device name database information.
pending-diff	Displays pending differences in the device name database information.
pwwn *pwwn-id*	Displays device name database information for a specific pWWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal digit.
session status	Displays the device name session status.
statistics	Displays device name database statistics.
status	Displays the device name database status.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To make use of fcaliases as device names instead of using the cryptic device name, add only one member per fcalias.

Examples

This example shows how to display the contents of the device alias database:

```
switch# show device-alias database
```

This example shows how to display all global fcaliases and all Virtual SAN (VSAN) dependent fcaliases:

```
switch# show device-alias name efg
```

This example shows how to display all global fcaliases and all VSAN dependent fcaliases:

```
switch# show device-alias statistics
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
device-alias name	Configures device alias names.
device-alias database	Configures device alias information.
device-alias distribute	Enables device alias CFS distribution.

Send comments to nx5000-docfeedback@cisco.com

show fabric-binding

To display configured fabric binding information, use the **show fabric-binding** command.

show fabric-binding {**database** [**active**] [**vsan** *vsan-id*] | **efmd statistics** [**vsan** *vsan-id*] | **statistics** [**vsan** *vsan-id*] | **status** [**vsan** *vsan-id*] | **violations** [**last** *number*]}

Syntax Description

database	Displays configured database information.
active	(Optional) Displays the active database configuration information.
vsan *vsan-id*	(Optional) Specifies the FICON-enabled Virtual SAN (VSAN) ID. The range is from 1 to 4093.
efmd statistics	Displays Exchange Fabric Membership Data (EFMD) statistics.
statistics	Displays fabric binding statistics.
status	Displays fabric binding status.
violations	Displays violations in the fabric binding configuration.
last *number*	(Optional) Specifies recent violations. The range is from 1 to 100.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured fabric binding database information:

```
switch# show fabric-binding database
```

This example shows how to display the active fabric binding information:

```
switch# show fabric-binding database active
```

This example shows how to display the active VSAN-specific fabric binding information:

```
switch# show fabric-binding database active vsan 61
```

This example shows how to displaythe configured VSAN-specific fabric binding information:

```
switch# show fabric-binding database vsan 4
```

This example shows how to display the fabric binding statistics:

```
switch# show fabric-binding statistics
```

This example shows how to display the fabric binding status for each VSAN:

```
switch# show fabric-binding status
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the EFMD statistics:

```
switch# show fabric-binding efmd statistics
```

This example shows how to display the EFMD statistics for a specified VSAN:

```
switch# show fabric-binding efmd statistics vsan 4
```

This example shows how to display the fabric binding violations:

```
switch# show fabric-binding violations
```

Related Commands

Command	Description
fabric-binding	Configures fabric binding in a VSAN.

Send comments to nx5000-docfeedback@cisco.com

show fc2

To display FC2 information, use the **show fc2** command.

show fc2 {**bind** | **classf** | **exchange** | **exchresp** | **flogi** | **nport** | **plogi** | **plogi_pwwn** | **port** [**brief**] | **socket** | **sockexch** | **socknotify** | **socknport** | **vsan**}

Syntax Description

bind	Displays FC2 socket bindings.
classf	Displays FC2 classf sessions.
exchange	Displays FC2 active exchanges.
exchresp	Displays FC2 active responder exchanges.
flogi	Displays FC2 FLOGI table.
nport	Displays FC2 local N ports.
plogi	Displays FC2 PLOGI sessions.
plogi_pwwn	Displays FC2 PLOGI pWWN entries.
port	Displays FC2 physical port table.
brief	(Optional) Displays FC2 physical port table in brief format.
socket	Displays FC2 active sockets.
sockexch	Displays FC2 active exchanges for each socket.
socknotify	Displays FC2 local N port PLOGI/LOGO notifications for each socket.
socknport	Displays FC2 local nports per each socket.
vsan	Displays the FC2 VSAN table.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the FC2 active socket information:

```
switch# show fc2 socket
```

This example shows how to display the FC2 socket binding information:

```
switch# show fc2 bind
```

This example shows how to display the FC2 local N port information:

```
switch# show fc2 nport
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the FC2 PLOGI session information:

```
switch# show fc2 plogi
```

This example shows how to display the FC2 physical port information:

```
switch# show fc2 port
```

This example shows how to display the FC2 local N port PLOGI notifications for each socket:

```
switch# show fc2 socknotify
```

This example shows how to display the FC2 local N ports for each socket:

```
switch# show fc2 socknport
```

This example shows how to display the FC2 VSAN table:

```
switch# show fc2 vsan
```

Send comments to nx5000-docfeedback@cisco.com

show fc-port-security

To display configured port security feature information, use the **show port-security** command.

show fc-port-security {**database** [**active** [**vsan** *vsan-id*]] | **fwwn** *fwwn-id* **vsan** *vsan-id* | **interface** {**fc** *slot/port* | **san-port-channel** *port*} **vsan** *vsan-id* | **vsan** *vsan-id* | **pending** [**vsan** *vsan-id*] | **pending-diff** [**vsan** *vsan-id*] | **session status** [**vsan** *vsan-id*] | **statistics** [**vsan** *vsan-id*] | **status** [**vsan** *vsan-id*] | **violations** [**last** *count* | **vsan** *vsan-id*]}

Syntax Description

database	Displays database-related port security information.
active	(Optional) Displays the activated database information.
vsan *vsan-id*	(Optional) Displays information for the specified database.
fwwn *fwwn-id*	Displays information for the specified fabric WWN.
interface	Displays information for an interface.
fc *slot/port*	Displays information for the specified Fibre Channel interface.
san-port-channel *port*	Displays information for the specified SAN port channel interface. The range is from 1 to 128.
pending	Displays the server address pending configuration.
pending-diff	Displays the server address pending configuration differences with the active configuration.
session status	Displays the port security session status on a per VSAN basis.
statistics	Displays port security statistics.
status	Displays the port security status on a per VSAN basis.
violations	Displays violations in the port security database.
last *count*	(Optional) Displays the last number of lines in the database. The range is from 1 to 100.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The **show fc-port-security** command was added. **Note** On a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to 4.2(1)N1(1), this command was known as the **show port-security** command.

Send comments to nx5000-docfeedback@cisco.com

Usage Guidelines

The access information for each port can be individually displayed. If you specify the fabric world wide name (fWWN) or interface options, all devices that are paired in the active database (at that point) with the given fWWN or the interface are displayed.

When you enter the **show fc-port-security** command with the **last** *number* option, only the specified number of entries that appear first are displayed.

Examples

This example shows how to display the contents of the port security database:

```
switch# show fc-port-security database
```

This example shows how to display the output of the active port security database in VSAN 1:

```
switch# show fc-port-security database vsan 1
```

This example shows how to display the active database:

```
switch# show fc-port-security database active
```

This example shows how to display the wildcard fWWN port security in VSAN 1:

```
switch# show fc-port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
```

This example shows how to display the configured fWWN port security in VSAN 1:

```
switch# show fc-port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
```

This example shows how to display the interface port information in VSAN 2:

```
switch# show fc-port-security database interface fc 2/1 vsan 2
```

This example shows how to display the port security statistics:

```
switch# show fc-port-security statistics
```

This example shows how to display the status of the active database and the autolearn configuration:

```
switch# show fc-port-security status
```

This example shows how to display the previous 100 violations:

```
switch# show fc-port-security violations
```

Related Commands

Command	Description
fc-port-security	Configures port security parameters.

Send comments to nx5000-docfeedback@cisco.com

show fcalias

To display the member name information in a Fibre Channel alias (fcalias), use the **show fcalias** command.

show fcalias [**name** *fcalias-name*] [**pending**] [**vsan** *vsan-id*]

Syntax Description

name *fcalias-name*	(Optional) Displays fcalias information for a specific name. The maximum length is 64.
pending	(Optional) Displays pending fcalias information.
vsan *vsan-id*	(Optional) Displays fcalias information for a VSAN. The range is from 1 to 4093.

Command Default

Displays a list of all global fcaliases and all VSAN-dependent fcaliases.

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

To make use of fcaliases as device names instead of using the cryptic device name, add only one member per fcalias.

Examples

This example shows how to display the fcalias configuration information:

```
switch# show fcalias vsan 1
```

Related Commands

Command	Description
fcalias name	Configures fcalias names.

Send comments to nx5000-docfeedback@cisco.com

show fcdomain

To display the Fibre Channel domain (fcdomain) information, use the **show fcdomain** command.

show fcdomain [**address-allocation** [**cache**] | **allowed** | **domain-list** | **fcid persistent** [**unused**] | **pending** [**vsan** *vsan-id***]** | **pending-diff** [**vsan** *vsan-id***]** | **session-status** [**vsan** *vsan-id***]** | **statistics** [**interface** {**fc** *slot/port* [**vsan** *vsan-id***]** } | **san-port-channel** *port* [**vsan** *vsan-id***]**] | **status** | **vsan** *vsan-id*]

Syntax Description

address-allocation	(Optional) Displays statistics for the FC ID allocation.
cache	(Optional) Reassigns the FC IDs for a device (disk or host) that exited and reentered the fabric for the principal switch. In the cache content, Virtual SAN (VSAN) refers to the VSAN that contains the device, WWN refers to the device that owned the FC IDs, and mask refers to a single or entire area of FC IDs.
allowed	(Optional) Displays a list of allowed domain IDs.
domain-list	(Optional) Displays a list of domain IDs provided by the principal switch.
fcid persistent	(Optional) Displays persistent FC IDs (across reboot).
unused	(Optional)
pending	(Optional) Displays the pending configuration.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is from 1 to 4093.
pending-diff	(Optional) Displays the difference between the running configuration and the pending configuration.
session-status	(Optional) Displays the last action performed by FC domain.
statistics	(Optional) Displays the statistics of FC domain.
interface	(Optional) Specifies an interface.
fc *slot/port*	(Optional) Specifies a Fibre Channel interface.
san-port-channel *port*	(Optional) Specifies a SAN port channel interface. The range is from 1 to 128.
status	(Optional) Displays all VSAN-independent information in FC domain.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When you enter the **show fcdomain** with no arguments, all VSANs are displayed. The VSANs should be active or you will get an error.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to display the fcdomain information for VSAN 1:

```
switch# show fcdomain vsan 1
```

This example shows how to display the fcdomain domain-list information for VSAN 76:

```
switch# show fcdomain domain-list vsan 76

Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

Table 9-1 describes the significant fields shown in the **show fcdomain domain-list** command output.

Table 9-1 show fcdomain Field Descriptions

Field	Description
Domain ID	Lists the domain IDs corresponding to the WWN.
WWN	Indicates the WWN of the switch (physical or virtual) that requested the corresponding domain ID.
Principal	Indicates which row of the display lists the WWN and domain ID of the principal switch in the VSAN.
Local	Indicates which row of the display lists the WWN and domain ID of the local switch (the switch where you entered the **show fcdomain domain-list** command).
Virtual (IVR)	Indicates which row of the display lists the WWN of the virtual switch used by the Inter-VSAN Routing (IVR) manager to obtain the domain ID.

This example shows how to display the allowed domain ID lists:

```
switch# show fcdomain allowed vsan 1
```

This example shows how to display the status of the CFS distribution for allowed domain ID lists:

```
switch# show fcdomain status
```

This example shows how to display the pending configuration changes:

```
switch# show fcdomain pending vsan 10
```

This example shows how to display the differences between the pending configuration and the current configuration:

```
switch# show fcdomain pending-diff vsan 10
```

This example shows how to display the status of the distribution session:

```
switch# show fcdomain session-status vsan 1
```

Related Commands

Command	Description
fcdomain	Configures the Fibre Channel domain feature.

Send comments to nx5000-docfeedback@cisco.com

show fcdroplatency

To display the configured Fibre Channel latency parameters, use the **show fcdroplatency** command.

show fcdroplatency [**network** | **switch**]

Syntax Description

network	(Optional) Displays the network latency in milliseconds.
switch	(Optional) Displays the switch latency in milliseconds.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured Fibre Channel latency parameters:

```
switch# show fcdroplatency
```

Related Commands

Command	Description
fcdroplatency	Configures the network and switch Fibre Channel drop latency time.

Send comments to nx5000-docfeedback@cisco.com

show fcflow stats

To display the configured Fibre Channel flow (fcflow) information, use the **show fcflow stats** command.

show fcflow stats [**aggregated** | **usage**] [**index** *flow-index*]

Syntax Description

aggregated	(Optional) Displays aggregated fcflow statistics.
usage	(Optional) Displays flow index usage.
index *flow-index*	(Optional) Specifies an fcflow index.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the aggregated fcflow details:

```
switch# show fcflow stats aggregated
```

This example shows how to display the fcflow details:

```
switch# show fcflow stats
```

This example shows how to display the fcflow index usage:

```
switch# show fcflow stats usage
```

Related Commands

Command	Description
fcflow stats	Configures fcflow statistics.

Send comments to nx5000-docfeedback@cisco.com

show fcid-allocation

To display the Fibre Channel area list of company IDs, use the **show fcid allocation** command.

show fcid-allocation area | **company-id-from-wwn** *wwn* [*company-id*]

Syntax Description

area	Displays the auto area list of company IDs.
company-id-from-wwn *wwn*	Displays the company ID from the specified world wide name (WWN).
company-id	(Optional) Company ID (also know as Organizational Unit Identifier, or OUI) to display.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the Fibre Channel area company list of company IDs:

```
switch# show fcid-allocation area
Fcid area allocation company id info:

    00:50:2E
    00:50:8B
    00:60:B0
    00:A0:B8
    00:E0:69
    00:E0:8B
    00:32:23 +


Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

Table 9-2 describes the significant fields shown in the display.

Table 9-2 show fcid-allocation area company Field Descriptions

Field	Description
+	Indicates a company ID added to the default list.
–	Indicates a company ID deleted from the default list.

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fcid-allocation	Adds a FCID to the default area company ID list.

Send comments to nx5000-docfeedback@cisco.com

show fcns database

To display the results of the discovery, or to display the name server database for a specified Virtual SAN (VSAN) or for all VSANs, use the **show fcns database** command.

show fcns database {**detail** [**vsan** *vsan-id*] | **domain** *domain-id* [**detail**] [**vsan** *vsan-range*] | **fcid** *fcid-id* [**detail**] **vsan** *vsan-range* | **local** [**detail**] [**vsan** *vsan-range*] | **vsan** *vsan-id*}

Syntax Description

detail	Displays all objects in each entry.
vsan *vsan-id*	(Optional) Displays entries for a specified VSAN ID. The range is from 1 to 4093.
domain *domain-id*	Displays entries in a domain.
detail	(Optional) Displays detailed entries for the domain.
fcid *fcid-id*	Displays entry for the given port.
local	Displays local entries.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The discovery can take several minutes to complete, especially if the fabric is large or if several devices are slow to respond.

Virtual enclosure ports can be viewed using the **show fcns database** command.

Examples

This example shows how to display the contents of the FCNS database:

```
switch# show fcns database
```

This example shows how to display the detailed contents of the FCNS database:

```
switch# show fcns database detail
```

This example shows how to display the management VSAN (VSAN 2):

```
switch# show fcns database vsan 2
```

This example shows how to display the database for all configured VSANs:

```
switch# show fcns database
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fcns	Specifies the configuration mode command for name server configuration.

Send comments to nx5000-docfeedback@cisco.com

show fcns statistics

To display the statistical information for a specified Virtual SAN (VSAN) or for all VSANs, use the **show fcns statistics** command.

show fcns statistics [**detail**] [**vsan** *vsan-id*]

Syntax Description

detail	(Optional) Displays detailed statistics.
vsan *vsan-id*	(Optional) Displays statistics for the specified VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the statistical information for a specified VSAN:

```
switch# show fcns statistics
```

Related Commands

Command	Description
fcns	Specifies the configuration mode command for name server configuration.

Send comments to nx5000-docfeedback@cisco.com

show fcoe

To display the status of Fibre Channel over Ethernet (FCoE) parameters on the switch, use the **show fcoe** command.

show fcoe

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the FCoE status:

```
switch# show fcoe
Global FCF details
        FCF-MAC is 00:0d:ec:a3:9d:80
        FC-MAP is 0e:fc:00
        FCF Priority is 128
        FKA Advertisement period for FCF is 8 seconds
switch#
```

Related Commands

Command	Description
fcoe fcf-priority	Configures the FCoE Initialization Protocol (FIP) priority value.
fcoe fcmap	Configures the FCoE MAC Address Prefix (FC MAP) used to associate the FCoE node (ENode).
fcoe fka-adv-period	Configures the time interval at which FIP keep alive (FKA) messages are transmitted to the MAC address of the ENode.
show fcoe database	Displays the FCoE database information.

Send comments to nx5000-docfeedback@cisco.com

show fcoe database

To display information about the Fibre Channel over Ethernet (FCoE) database, use the **show fcoe database** command.

show fcoe database

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the FCoE database:

```
switch# show fcoe database

------------------------------------------------------------------------------
INTERFACE       FCID            PORT NAME               MAC ADDRESS
------------------------------------------------------------------------------
vfc1            0x580016        10:00:00:00:07:f8:0e:45 00:00:00:13:05:01
vfc1            0x580017        10:00:00:00:07:f8:21:bf 00:00:00:13:05:01
vfc2            0x580020        10:00:00:00:07:f8:0e:46 00:00:00:13:05:02
vfc2            0x580033        10:00:00:00:07:f8:21:c0 00:00:00:13:05:02
vfc4            0x58001e        10:00:00:00:07:f8:0e:48 00:00:00:13:05:04
vfc4            0x580031        10:00:00:00:07:f8:21:c2 00:00:00:13:05:04
vfc5            0x58001d        10:00:00:00:07:f8:0e:49 00:00:00:13:05:05
vfc5            0x580030        10:00:00:00:07:f8:21:c3 00:00:00:13:05:05
vfc6            0x58001c        10:00:00:00:07:f8:0e:4a 00:00:00:13:05:06
vfc6            0x58002f        10:00:00:00:07:f8:21:c4 00:00:00:13:05:06
vfc7            0x58001b        10:00:00:00:07:f8:0e:4b 00:00:00:13:05:07
vfc7            0x58002e        10:00:00:00:07:f8:21:c5 00:00:00:13:05:07
vfc8            0x58001a        10:00:00:00:07:f8:0e:4c 00:00:00:13:05:08
vfc8            0x58002d        10:00:00:00:07:f8:21:c6 00:00:00:13:05:08
vfc9            0x580019        10:00:00:00:07:f8:0e:4d 00:00:00:13:05:09
vfc9            0x58002c        10:00:00:00:07:f8:21:c7 00:00:00:13:05:09
vfc10           0x580018        10:00:00:00:07:f8:0e:4e 00:00:00:13:05:0a
vfc10           0x58002a        10:00:00:00:07:f8:21:c8 00:00:00:13:05:0a
vfc11           0x580023        10:00:00:00:07:f8:0e:4f 00:00:00:13:05:0b
vfc11           0x580036        10:00:00:00:07:f8:21:c9 00:00:00:13:05:0b
vfc12           0x580022        10:00:00:00:07:f8:0e:50 00:00:00:13:05:0c
vfc12           0x580035        10:00:00:00:07:f8:21:ca 00:00:00:13:05:0c
vfc13           0x580021        10:00:00:00:07:f8:0e:51 00:00:00:13:05:0d
vfc13           0x580034        10:00:00:00:07:f8:21:cb 00:00:00:13:05:0d
vfc14           0x58002b        10:00:00:00:07:f8:0e:52 00:00:00:13:05:0e
vfc14           0x58003d        10:00:00:00:07:f8:21:cc 00:00:00:13:05:0e
vfc15           0x580029        10:00:00:00:07:f8:0e:53 00:00:00:13:05:0f
vfc15           0x58003c        10:00:00:00:07:f8:21:cd 00:00:00:13:05:0f
```

Send comments to nx5000-docfeedback@cisco.com

```
vfc16           0x580028        10:00:00:00:07:f8:0e:54 00:00:00:13:05:10
vfc16           0x58003b        10:00:00:00:07:f8:21:ce 00:00:00:13:05:10
vfc17           0x580027        10:00:00:00:07:f8:0e:55 00:00:00:13:05:11
vfc17           0x580039        10:00:00:00:07:f8:21:cf 00:00:00:13:05:11
vfc18           0x580026        10:00:00:00:07:f8:0e:56 00:00:00:13:05:12
vfc18           0x58003a        10:00:00:00:07:f8:21:d0 00:00:00:13:05:12
vfc19           0x580025        10:00:00:00:07:f8:0e:57 00:00:00:13:05:13
vfc19           0x580038        10:00:00:00:07:f8:21:d1 00:00:00:13:05:13
vfc20           0x580024        10:00:00:00:07:f8:0e:58 00:00:00:13:05:14
switch#
```

Related Commands

Command	Description
fcoe fcf-priority	Configures the FCoE Initialization Protocol (FIP) priority value.
fcoe fcmap	Configures the FCoE MAC Address Prefix (FC MAP) used to associate the FCoE node (ENode).
fcoe fka-adv-period	Configures the time interval at which FIP keep alive (FKA) messages are transmitted to the MAC address of the ENode.
show fcoe	Displays the status of the FCoE parameters.

Send comments to nx5000-docfeedback@cisco.com

show fcroute

To view specific information about existing Fibre Channel and Fabric Shortest Path First (FSPF) configurations, use the **show fcroute** command.

show fcroute {**distance** | **label** [*label*] **vsan** *vsan-id* | **multicast** [*fc-id* **vsan** *vsan-id* | **vsan** *vsan-id*] | **summary** [**vsan** *vsan-id*] | **unicast** [[*host*] *fc-id fc-mask* **vsan** *vsan-id* | **vsan** *vsan-id*]}

Syntax Description

distance	Displays the FC route preference.
label	Displays label routes.
label	(Optional) Label routes for the specified label.
vsan *vsan-id*	(Optional) Specifies the ID of the VSAN (from 1 to 4093).
multicast	Displays FC multicast routes.
fc-id	(Optional) Fibre Channel ID.
summary	Displays the FC routes summary.
unicast	Displays FC unicast routes.
host	Unicast routes for the specified host.
fc-mask	Unicast routes for hosts that match the range of FCIDs that are specified by the mask.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the number of routes are displayed in the command output, both visible and hidden routes are included in the total number of routes.

Examples

This example shows how to display the administrative distance:

```
switch# show fcroute distance
```

This example shows how to display the multicast routing information:

```
switch# show fcroute multicast
```

This example shows how to display the FCID information for a specified VSAN:

```
switch# show fcroute multicast vsan 3
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the FCID and interface information for a specified VSAN:

```
switch# show fcroute multicast 0xffffff vsan 2
```

This example shows how to display the unicast routing information:

```
switch# show fcroute unicast
```

This example shows how to display the unicast routing information for a specified VSAN:

```
switch# show fcroute unicast vsan 4
```

This example shows how to display the unicast routing information for a specified FCID:

```
switch# show fcroute unicast 0x040101 0xffffff vsan 4
```

This example shows how to display the route database information:

```
switch# show fcroute summary
```

This example shows how to display the route database information for a specified VSAN:

```
switch# show fcroute summary vsan 4
```

Related Commands

Command	Description
fcroute	Configures Fibre Channel routes and activates policy routing.

Send comments to nx5000-docfeedback@cisco.com

show fcs

To display the status of the fabric configuration, use the **show fcs** commands.

show fcs {**database** [**vsan** *vsan-id*] | **ie** [**nwwn** *wwn* | **vsan** *vsan-id*] | **platform** {**name** *string* | **vsan** *vsan-id*} | **port** {**pwwn** *wwn* | **vsan** *vsan-id*} | **statistics vsan** *vsan-id* | **vsan**}

Syntax Description

database	Displays local database of frame check sequence (FCS).
vsan *vsan-id*	(Optional) Specifies a Virtual SAN (VSAN) ID. The range is from 1 to 4093.
ie	Displays interconnect element objects information.
nwwn *wwn*	(Optional) Specifies a node WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
platform	Displays platform objects information.
name *string*	(Optional) Specifies a platform name. The name can be a maximum of 255 characters.
port	Displays port objects information.
pwwn *wwn*	Specifies a port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
statistics	Displays statistics for FCS packets.
vsan	Displays list of all the VSANs.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the FCS database information:

```
switch# show fcs database
```

This example shows how to display the interconnect element object information for a specific VSAN:

```
switch# show fcs ie vsan 1
```

This example shows how to display the interconnect element object information for a specific WWN:

```
switch# show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1
```

This example shows how to display the platform information:

```
switch# show fcs platform name SamplePlatform vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how display to the platform information within a specified VSAN:

```
switch# show fcs platform vsan 1
```

This example shows how to display the FCS port information within a specified VSAN:

```
switch# show fcs port vsan 24
```

This example shows how to display the ports within a specified WWN:

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
```

This example shows how to display the FCS statistics:

```
switch# show fcs statistics
```

Related Commands

Command	Description
fcs	Configures FCS platform attributes.

Send comments to nx5000-docfeedback@cisco.com

show fcsp

To display the status of the Fibre Channel Security Protocol (FC-SP) configuration, use the **show fcsp** commands.

show fcsp [**asciiwwn** *ascii-wwn* | **dhchap** [**database**] | **interface** {**fc** *slot*/*port* | **vfc** *vfc-id*} [**statistics** | **wwn**]]

Syntax Description

asciiwwn *ascii-wwn*	(Optional) Displays the ASCII representation of the WWN used with authentication, authorization, and accounting (AAA) server.
dhchap	(Optional) Displays the DHCHAP hash algorithm status.
database	(Optional) Displays the contents of the local DHCHAP database.
interface	(Optional) Displays the FC-SP settings for a Fibre Channel or Fibre Channel interface.
fc *slot*/*port*	Specifies a Fibre Channel interface.
vfc *vfc-id*	(Optional) Specifies a virtual Fibre Channel interface.
statistics	(Optional) Displays the statistics for the specified interface.
wwn	(Optional) Displays the FC-SP identity of the other device.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the DHCHAP configurations in FC interfaces:

```
switch# show fcsp interface fc2/3
```

This example shows how to display the DHCHAP statistics for an FC interface:

```
switch# show fcsp interface fc2/3 statistics
```

This example shows how to display the FC-SP WWN of the device connected through a specified interface:

```
switch# show fcsp interface fc 2/1 wwn
```

This example shows how to display the hash algorithm and DHCHAP groups configured for the local switch:

```
switch# show fcsp dhchap
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the DHCHAP local password database:

```
switch# show fcsp dhchap database
```

This example shows how to display the ASCII representation of the device WWN:

```
switch# show fcsp asciiwwn 30:11:bb:cc:dd:33:11:22
```

Related Commands

Command	Description
fcsp enable	Enables the FC-SP feature for this switch.

Send comments to nx5000-docfeedback@cisco.com

show fctimer

To display the Fibre Channel timers (fctimer), use the **show fctimer** command.

show fctimer [**d_s_tov** [**vsan** *vsan-id*] | **e_d_tov** [**vsan** *vsan-id*] | **f_s_tov** [**vsan** *vsan-id*] | **r_a_tov** [**vsan** *vsan-id*] | **last action status** | **pending** | **pending-diff** | **session status** | **status** | **vsan** *vsan-id*]

Syntax Description

d_s_tov	(Optional) Displays the distributed services time out value (D_S_TOV) in milliseconds.
vsan *vsan-id*	(Optional) Displays information for a Virtual SAN (VSAN). The range is from 1 to 4093.
e_d_tov	(Optional) Displays the error detection timeout value (E_D_TOV) in milliseconds.
f_s_tov	(Optional) Displays the fabric stability timeout value (F_S_TOV) in milliseconds.
r_a_tov	(Optional) Displays the resource allocation time out value (R_A_TOV) in milliseconds.
last action status	(Optional) Displays the status of the last Cisco Fabric Services (CFS) commit or discard operation.
pending	(Optional) Displays the status of pending fctimer commands.
pending-diff	(Optional) Displays the difference between the pending database and running configuration.
session status	(Optional) Displays the state of the fctimer CFS session.
status	(Optional) Displays the Fibre Channel timer status.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured global TOVs:

```
switch# show fctimer
```

This example shows how to display the configured TOVs for a specified VSAN:

```
switch# show fctimer vsan 10
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fctimer	Configures fctimer parameters.

Send comments to nx5000-docfeedback@cisco.com

show fdmi

To display the Fabric-Device Management Interface (FDMI) database information, use the **show fdmi** command.

show fdmi database [**detail** [**hba-id** {*hba-id* **vsan** *vsan-id*} | **vsan** *vsan-id*] | **vsan** *vsan-id*] | **suppress-updates**

Syntax Description

database	Displays the FDMI database contents.
detail	(Optional) Specifies detailed FDMI information.
hba-id *hba-id*	(Optional) Displays detailed information for the specified host bus adapter (HBA) entry.
vsan *vsan-id*	(Optional) Specifies FDMI information for the specified Virtual SAN (VSAN). The range is from 1 to 4093.
suppress-updates	Displays the VSANs that are configured to suppress updates.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all HBA management servers:

```
switch# show fdmi database
```

This example shows how to display the VSAN1-specific FDMI information:

```
switch# show fdmi database detail vsan 1
```

This example shows how to display the details for the specified HBA entry:

```
switch# show fdmi database detail Hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1
```

Related Commands

Command	Description
fdmi suppress-updates	Suppresses FDMI updates.

Send comments to nx5000-docfeedback@cisco.com

show flogi

To list all the fabric login (FLOGI) sessions through all interfaces across all Virtual SAN (VSANs), use the **show flogi** command.

show flogi {**auto-area-list**} | **database** {**fcid** *fcid-id* | **interface** {**fc** *slot*/*port* | **vfc** *vfc-id*} | **vsan** *vsan-id*}

Syntax Description

auto-area-list	Displays the list of Organizational Unit Identifiers (OUIs) that are allocated areas.
database	Displays information about FLOGI sessions.
fcid *fcid-id*	Displays FLOGI database entries based on the FCID allocated. The format is *0xhhhhhh*.
interface	Displays FLOGI database entries based on the logged in interface.
fc *slot*/*port*	Specifies the Fibre Channel or virtual Fibre Channel interface by slot and port number.
vfc *vfc-id*	Specifies a virtual Fibre Channel interface.
vsan *vsan-id*	Displays FLOGI database entries based on the VSAN ID. The range is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The output of this command is sorted by interface numbers and then by VSAN IDs.

In a Fibre Channel fabric, each host or disk requires an FCID. Use the **show flogi database** command to verify if a storage device is displayed in the fabric login (FLOGI) table as in the examples below. If the required device is displayed in the FLOGI table, the fabric login is successful. Examine the FLOGI database on a switch that is directly connected to the host HBA and connected ports.

Examples

This example shows how to display the details on the FLOGI database:

```
switch# show flogi database
```

This example shows how to display the FLOGI interface:

```
switch# show flogi database interface fc 2/3
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the FLOGI VSAN:

```
switch# show flogi database vsan 1
```

This example shows how to display the FLOGI for a specific FCID:

```
switch# show flogi database fcid 0xef02e2
```

Related Commands

Command	Description
show fcns database	Displays all the local and remote name server entries.

Send comments to nx5000-docfeedback@cisco.com

show fspf

To display global Fibre Shortest Path First (FSPF) routing information, use the **show fspf** command.

show fspf [**database** [**vsan** *vsan-id*] [**detail** | **domain** *domain-id* **detail**] | **interface** | **vsan** *vsan-id* **interface** {**fc** *slot*/*port* | **san-port-channel** *port-channel*}]

Syntax Description

database	(Optional) Displays the FSPF link state database.
vsan *vsan-id*	(Optional) Specifies the Virtual SAN (VSAN) ID. The range is from 1 to 4093.
detail	(Optional) Displays detailed FSPF information.
domain *domain-id*	(Optional) Specifies the domain of the database. The range is from 0 to 255.
interface	(Optional) Specifies the FSPF interface.
fc *slot*/*port*	Specifies the Fibre Channel interface to configure.
san-port-channel *port-channel*	Specifies the port channel interface. The range is from 1 to 256.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you enter the command without parameters, all the entries in the database are displayed.

Examples

This example shows how to display the FSPF interface information:

```
switch# show fspf interface vsan 1 fc2/1
```

This example shows how to display the FSPF database information:

```
switch# show fspf database vsan 1
```

This command shows how to display the FSPF information for a specified VSAN:

```
switch# show fspf vsan 1
```

Related Commands

Command	Description
fspf	Configures FSPF.

Send comments to nx5000-docfeedback@cisco.com

show in-order-guarantee

To display the present configured state of the in-order delivery feature, use the **show in-order-guarantee** command.

show in-order-guarantee

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the present configuration status of the in-order delivery feature:

```
switch# show in-order-guarantee
```

Related Commands

Command	Description
in-order-guarantee	Enables in-order delivery.

Send comments to nx5000-docfeedback@cisco.com

show interface fcoe

To display information about the Fibre Channel over Ethernet (FCoE) for an interface, use the **show interface fcoe** command.

show interface [*interface number*] **fcoe**

Syntax Description

interface	(Optional) Interface, either Ethernet or EtherChannel.
number	Interface number. The number can be one of the following: • The Ethernet interface slot and the port number within the slot. The slot number range is from 1 to 255, and the port number range is from 1/255. • The EtherChannel number. The range is from 1 to 4096.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the FCoE information for Ethernet interfaces:

```
switch# show interface fcoe
Ethernet1/1 is FCoE UP
Ethernet1/2 is FCoE UP
Ethernet1/3 is FCoE UP
Ethernet1/4 is FCoE UP
Ethernet1/5 is FCoE UP
Ethernet1/6 is FCoE UP
Ethernet1/7 is FCoE UP
Ethernet1/8 is FCoE UP
Ethernet1/9 is FCoE UP
Ethernet1/10 is FCoE UP
Ethernet1/11 is FCoE down
Ethernet1/12 is FCoE down
Ethernet1/13 is FCoE UP
Ethernet1/14 is FCoE UP
Ethernet1/15 is FCoE down
Ethernet1/16 is FCoE down
Ethernet1/17 is FCoE UP
Ethernet1/18 is FCoE down
Ethernet1/19 is FCoE UP
Ethernet1/20 is FCoE UP
Ethernet1/21 is FCoE UP
Ethernet1/22 is FCoE UP
Ethernet1/23 is FCoE UP
Ethernet1/24 is FCoE UP
```

Send comments to nx5000-docfeedback@cisco.com

```
Ethernet1/25 is FCoE UP
Ethernet1/26 is FCoE UP
Ethernet1/27 is FCoE UP
Ethernet1/28 is FCoE UP
Ethernet1/29 is FCoE UP
Ethernet1/30 is FCoE UP
Ethernet1/31 is FCoE UP
Ethernet1/32 is FCoE UP
Ethernet1/33 is FCoE UP
    vfc1 is Up
        FCID is 0x580016
        PWWN is 10:00:00:00:07:f8:0e:45
        MAC addr is 00:00:00:13:05:01
        FCID is 0x580017
        PWWN is 10:00:00:00:07:f8:21:bf
        MAC addr is 00:00:00:13:05:01
    vfc2 is Up
        FCID is 0x580020
        PWWN is 10:00:00:00:07:f8:0e:46
        MAC addr is 00:00:00:13:05:02
        FCID is 0x580033
        PWWN is 10:00:00:00:07:f8:21:c0
        MAC addr is 00:00:00:13:05:02
    vfc4 is Up
        FCID is 0x58001e
        PWWN is 10:00:00:00:07:f8:0e:48
        MAC addr is 00:00:00:13:05:04
        FCID is 0x580031
        PWWN is 10:00:00:00:07:f8:21:c2
        MAC addr is 00:00:00:13:05:04
    vfc5 is Up
        FCID is 0x58001d
        PWWN is 10:00:00:00:07:f8:0e:49
        MAC addr is 00:00:00:13:05:05
        FCID is 0x580030
        PWWN is 10:00:00:00:07:f8:21:c3
        MAC addr is 00:00:00:13:05:05
    vfc6 is Up
        FCID is 0x58001c
        PWWN is 10:00:00:00:07:f8:0e:4a
        MAC addr is 00:00:00:13:05:06
        FCID is 0x58002f
        PWWN is 10:00:00:00:07:f8:21:c4
        MAC addr is 00:00:00:13:05:06
Ethernet1/34 is FCoE down
Ethernet1/35 is FCoE UP
Ethernet1/36 is FCoE UP
Ethernet1/37 is FCoE down
Ethernet1/38 is FCoE UP
Ethernet1/39 is FCoE down
Ethernet1/40 is FCoE UP
Ethernet3/1 is FCoE down
Ethernet3/2 is FCoE down
Ethernet3/3 is FCoE UP
Ethernet3/4 is FCoE UP
Ethernet3/5 is FCoE UP
Ethernet3/6 is FCoE UP
port-channel1 is FCoE down
port-channel3 is FCoE UP
port-channel5 is FCoE down
port-channel6 is FCoE down
port-channel12 is FCoE down
port-channel15 is FCoE down
port-channel20 is FCoE down
```

Send comments to nx5000-docfeedback@cisco.com

```
port-channel24 is FCoE UP
port-channel25 is FCoE UP
port-channel33 is FCoE down
port-channel41 is FCoE down
port-channel44 is FCoE down
port-channel48 is FCoE down
--More--
switch#
```

This example shows how to display the FCoE information for a specific Ethernet interface:

```
switch# show interface ethernet 1/21 fcoe
Ethernet1/21 is FCoE UP
switch#
```

This example shows how to display the FCoE information for a specific EtherChannel interface:

```
switch# show interface port-channel 3 fcoe
port-channel3 is FCoE UP
switch#
```

Related Commands

Command	Description
show fcoe	Displays the status of the FCoE parameters.

Send comments to nx5000-docfeedback@cisco.com

show lldp

To display information about the Link Layer Discovery Protocol (LLDP) configuration on the switch, use the **show lldp** command.

show lldp {**interface** {**ethernet** *slot/port* | **mgmt** *intf-no*} | **neighbors** [**detail** | **interface**] | **timers** | **traffic** [**interface** {**ethernet** *slot/port* | **mgmt** *intf-no*}]}

Syntax Description

interface	Displays LLDP interface information, or LLDP neighbor information on an interface.
ethernet *slot/port*	Displays the configuration information of the Ethernet IEEE 802.3z interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
mgmt *intf-no*	Displays the configuration information of the management interface. The management interface number is 0.
neighbors	Displays information about LLDP neighbors.
detail	(Optional) Displays the detailed information about LLDP neighbors.
timers	Displays information about LLDP timers.
traffic	Displays the LLDP counters configured on the switch.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display LLDP interface information:

```
switch# show lldp traffic interface ethernet 1/1
LLDP interface traffic statistics:

    Total frames transmitted: 7490
    Total entries aged: 0
    Total frames received: 7458
    Total frames received in error: 0
    Total frames discarded: 0
    Total unrecognized TLVs: 0
switch#
```

This example shows how to display LLDP management interface information:

```
switch# show lldp traffic interface mgmt 0
LLDP interface traffic statistics:

    Total frames transmitted: 0
    Total entries aged: 0
```

Send comments to nx5000-docfeedback@cisco.com

```
    Total frames received: 0
    Total frames received in error: 0
    Total frames discarded: 0
    Total unrecognized TLVs: 0
switch#
```

This example shows how to display LLDP timers configured on the switch:

```
switch# show lldp timers
LLDP Timers:

    Holdtime in seconds: 120
    Reinit-time in seconds: 2
    Transmit interval in seconds: 30
switch#
```

This example shows how to display LLDP neighbor information:

```
switch# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Local Intf  Chassis ID        Port ID        Hold-time   Capability
Eth1/1      000d.eca3.6080    Eth1/1            120      B
Eth1/2      000d.eca3.6080    Eth1/2            120      B
Eth1/3      000d.eca3.6080    Eth1/3            120      B
Eth1/4      000d.eca3.6080    Eth1/4            120      B
Eth1/7      000d.ecf2.0880    Eth1/7            120      B
Eth1/8      000d.ecf2.0880    Eth1/8            120      B
Eth1/9      000d.ecf2.0b40    Eth1/9            120      B
Eth1/10     000d.ecf2.0b40    Eth1/10           120      B
switch#
```

This example shows how to display LLDP information for a specified interface:

```
switch# show lldp interface ethernet 1/1
Interface Information:
  Enable (tx/rx/dcbx): Y/Y/Y    Port Mac address: 00:0d:ec:b2:30:c8

Peer's LLDP TLVs:
Type Length Value
---- ------ -----
001  007    04000dec a36080
002  007    05457468 312f31
003  002    0078
004  009    4e354b2d 506f7274 00
005  013    45756765 6e652d4e 354b2d32 00
006  010    4e354b2d 53776974 6368
007  004    00040004
008  012    05010ac1 8303021a 00000000
128  055    001b2102 020a0000 00000001 00000001 06060000 80000808 080a0000
            80008906 001b2108 04110000 80000001 00003232 00000000 000002
128  005    00014201 01
128  006    0080c201 0001
000  000
switch#
```

This example shows how to display LLDP traffic information:

```
switch# show lldp traffic
LLDP traffic statistics:

    Total frames transmitted: 89743
    Total entries aged: 0
    Total frames received: 59300
```

Send comments to nx5000-docfeedback@cisco.com

```
    Total frames received in error: 0
    Total frames discarded: 0
    Total unrecognized TLVs: 0
switch#
```

Related Commands

Command	Description
lldp	Configures the global LLDP options on the switch.
lldp (Interface)	Configures the LLDP feature on an interface.

Send comments to nx5000-docfeedback@cisco.com

show loadbalancing

To display load balancing status for specific unicast flows, use the **show loadbalancing** command.

show loadbalancing vsan *vsan-id source-fcid dest-fcid* [*exchange-id*]

Syntax Description

vsan *vsan-id*	Displays Fabric login (FLOGI) database entries based on the FCID allocated. The format is 0xhhhhhh.
source-fcid	Displays the load balancing status for the specified source FCID. The format is 0xhhhhhh.
dest-fcid	Displays the load balancing status for the specified destination FCID. The format is 0xhhhhhh.
exchange-id	(Optional) Displays the load balancing status for the specified exchange. The format is 0xhhhhhh.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the load-balancing information for the specified source and destination in VSAN 3:

```
switch# show loadbalancing vsan 3 0x3345 0x2546
```

Send comments to nx5000-docfeedback@cisco.com

show npv flogi-table

To display the information about N port virtualization (NPV) Fabric login (FLOGI) session, use the **show npv flogi-table** command.

show npv flogi-table

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show npv flogi-table** command is available only when the switch is in NPV mode.

Examples

This example shows how to display the information on NPV FLOGI session:

```
switch# show npv flogi-table
```

Related Commands

Command	Description
show npv status	Displays the NPV current status.

Send comments to nx5000-docfeedback@cisco.com

show npv status

To display the N port virtualization (NPV) current status, use the **show npv status** command.

show npv status

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show npv status** command is available only when the switch is in NPV mode.

Examples

This example shows how to display the current status of NPV:

```
switch# show npv status
```

Related Commands

Command	Description
show npv flogi-table	Displays the information about NPV FLOGI session.

Send comments to nx5000-docfeedback@cisco.com

show npv traffic-map

To display N port virtualization (NPV) traffic maps, use the **show npv traffic-map** command.

show npv traffic-map

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The **show npv traffic-map** command is available only when the switch is in NPV mode.

Examples

This example shows how to display the current status of NPV:

```
switch# show npv traffic-map
```

Related Commands

Command	Description
show npv flogi-table	Displays the information about an NPV FLOGI session.

Send comments to nx5000-docfeedback@cisco.com

show port index-allocation

To display port index allocation information, use the **show port index-allocation** command.

show port index-allocation [**startup**]

Syntax Description

startup	(Optional) Displays port index allocation information at startup.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

On a switch where the maximum number of port indexes is 256, any module that exceeds that limit does not power up. There is no startup module index distribution for the Cisco Nexus 5000 Series switch.

Examples

This example shows how to display port index allocation information:

```
switch# show port index-allocation
```

Send comments to nx5000-docfeedback@cisco.com

show rlir

To display Registered Link Incident Report (RLIR) information, use the **show rlir** command.

show rlir {**erl** [**vsan** *vsan-id*] | **history** | **recent** {**interface fc** *slot*/*port* | **portnumber** *port*} | **statistics** [**vsan** *vsan-id*]}

Syntax Description

erl	Displays the Established Registration List.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is from 1 to 4093.
history	Displays the link incident history.
recent	Displays recent link incidents.
interface fc *slot*/*port*	Specifies a Fibre Channel interface.
portnumber *port*	Displays RLIR information for the specified port number.
statistics	Displays RLIR statistics for all VSANs or the specified VSAN.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the RLIR information for VSAN 1:

```
switch# show rlir erl vsan 1
```

This example shows how to display the RLIR statistics:

```
switch# show rlir statistics vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

show rscn

To display Registered State Change Notification (RSCN) information, use the **show rscn** command.

show rscn {**event-tov vsan** *vsan-id* | **pending vsan** *vsan-id* | **pending-diff vsan** *vsan-id* | **scr-table** [**vsan** *vsan-id*] | **session status vsan** *vsan-id* | **statistics** [**vsan** *vsan-id*]}

Syntax Description

event-tov	Displays the event timeout value.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 1 to 4093.
pending	Displays the pending configuration.
pending-diff	Displays the difference between the active and the pending configuration.
scr-table	Displays the State Change Registration (SCR) table.
session status	Displays the RSCN session status.
statistics	Displays RSCN statistics.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The SCR table cannot be configured. It is only populated if one or more N ports send SCR frames to register for RSCN information. If the **show rscn scr-table** command does not return any entries, no N port is interested in receiving RSCN information.

Examples

This example shows how to display the RSCN information:

```
switch# show rscn scr-table vsan 1
```

This example shows how to display the RSCN statistics:

```
switch# show rscn statistics vsan 1
```

This example shows how to display he RSCN event timeout value configured on VSAN 1:

```
switch# show rscn event-tov vsan 1
```

This example shows how to display the difference between the active RSCN configuration and the pending RSCN configuration on VSAN 1:

```
switch# show rscn pending-diff vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
rscn	Configures a registered state change notification (RSCN).

Send comments to nx5000-docfeedback@cisco.com

show san-port-channel

To view information about existing SAN port channel configurations, use the **show san-port-channel** command.

show san-port-channel {**compatibility-parameters** | **consistency** [**detail**] | **database** [**interface san-port-channel** *port*] | **summary** | **usage**}

Syntax Description

compatibility-parameters	Displays compatibility parameters.
consistency	Displays the database consistency information of all modules.
detail	(Optional) Displays detailed database consistency information.
database	Displays SAN port channel database information.
interface san-port-channel *port*	(Optional) Specifies the SAN port channel number. The range is from 1 to 256.
summary	Displays the SAN port channel summary.
usage	Displays the SAN port channel number usage.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the SAN port channel summary:

```
switch# show san-port-channel summary
```

This example shows how to display the SAN port channel compatibility parameters:

```
switch# show san-port-channel compatibility-parameters
```

This example shows how to display the SAN port channel database:

```
switch# show san-port-channel database
```

This example shows how to display the consistency status of the SAN port channel database:

```
switch# show san-port-channel consistency
```

This example shows how to display detailed information about the consistency status of the SAN port channel database:

```
switch# show san-port-channel consistency detail
```

This example shows how to display details of the used and unused SAN port channel numbers:

```
switch# show san-port-channel usage
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
san-port-channel persistent	Converts an autocreated SAN port channel to a persistent SAN port channel.

Send comments to nx5000-docfeedback@cisco.com

show scsi-target

To display information about existing SCSI target configurations, use the **show scsi-target** command.

show scsi-target {**auto-poll** | **custom-list** | **devices** [**vsan** *vsan-id*] [**fcid** *fcid-id*] | **disk** [**vsan** *vsan-id*] [**fcid** *fcid-id*] | **lun** [**vsan** *vsan-id*] [**fcid** *fcid-id*] [**os** [**aix** | **all** | **hpux** | **linux** | **solaris** | **windows**] | **pwwn** | **status** | **tape** [**vsan** *vsan-id*] [**fcid** *fcid-id*] | **vsan** *vsan-id*}

Syntax Description

auto-poll	Displays SCSI target auto polling information.
custom-list	Displays customized discovered targets.
devices	Displays discovered SCSI target devices information
vsan *vsan-id*	(Optional) Specifies the Virtual SAN (VSAN) ID. The range is from 1 to 4093.
fcid *fcid-id*	(Optional) Specifies the FCID of the SCSI target to display.
disk	Displays discovered disk information.
lun	Displays discovered SCSI target logical unit number (LUN) information.
os	(Optional) Discovers the specified operating system.
aix	(Optional) Specifies the AIX operating system.
all	(Optional) Specifies all operating systems.
hpux	(Optional) Specifies the HPUX operating system.
linux	(Optional) Specifies the Linux operating system.
solaris	(Optional) Specifies the Solaris operating system.
windows	(Optional) Specifies the Windows operating system.
pwwn	Displays discovered pWWN information for each operating system.
status	Displays the SCSI target discovery status.
tape	Displays discovered tape information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use the **show scsi-target auto-poll** command to verify automatic discovery of online SCSI targets.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to display the status of a SCSI discovery:

```
switch# show scsi-target status
```

This example shows how to display the customized discovered targets:

```
switch# show scsi-target custom-list
```

This example shows how to display the discovered disk information:

```
switch# show scsi-target disk
```

This example shows how to display the discovered LUNs for all operating systems:

```
switch# show scsi-target lun os all
```

This example shows how to display the discovered LUNs for the Solaris operating system:

```
switch# show scsi-target lun os solaris
```

This example shows how to display the auto-polling information:

```
switch# show scsi-target auto-poll
```

This example shows how to display the port WWN that is assigned to each operating system (Windows, AIX, Solaris, Linux, or HPUX):

```
switch# show scsi-target pwwn
```

Related Commands

Command	Description
scsi-target	Configures SCSI target discovery.

Send comments to nx5000-docfeedback@cisco.com

show topology

To display topology information for connected SAN switches, use the **show topology** command.

show topology [**vsan** *vsan-id*]

Syntax Description		
	vsan *vsan-id*	(Optional) Displays information for a VSAN. The range is from 1 to 4093.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display topology information:

```
switch# show topology
```

Send comments to nx5000-docfeedback@cisco.com

show trunk protocol

To display the trunk protocol status, use the **show trunk protocol** command.

show trunk protocol

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the trunk protocol status:

```
switch# show trunk protocol
switch#
```

Related Commands

Command	Description
trunk protocol enable	Configures the trunking protocol for Fibre Channel interfaces.

Send comments to nx5000-docfeedback@cisco.com

show vlan fcoe

To display information about the Fibre Channel over Ethernet (FCOE) VLAN to Virtual SAN (VSAN) mappings, use the **show vlan fcoe** command.

show vlan fcoe

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the FCoE VLAN to VSAN mappings on the switch:

```
switch# show vlan fcoe
VLAN      VSAN      Status
--------  --------  --------
331       331       Operational
332       332       Operational
333       333       Operational
334       334       Operational
335       335       Non-operational
336       336       Operational
337       337       Operational
switch#
```

Related Commands

Command	Description
fcoe vsan	Maps a FCoE VLAN to a VSAN.

Send comments to nx5000-docfeedback@cisco.com

show vsan

To display information about configured Virtual SAN (VSAN), use the **show vsan** command.

show vsan [*vsan-id* [**membership**] | **membership** [**interface** {**fc** *slot*/*port* | **san-port-channel** *port* | **vfc** *vfc-id*}] | **usage**]

Syntax Description

vsan-id	(Optional) Information for the specified VSAN ID. The range is from 1 to 4094.
membership	(Optional) Displays membership information.
interface	(Optional) Specifies the interface type.
fc *slot*/*port*	Specifies a Fibre Channel interface.
san-port-channel *port*	Specifies a SAN port channel interface specified by the port channel number.
vfc *vfc-id*	Specifies a virtual Fibre Channel interface.
usage	(Optional) Displays VSAN usage in the system.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.2(1)N1(1)	The range of the VSAN ID is extended to 4094.

Usage Guidelines

When you enter the **show vsan membership interface** command, interface information appears for interfaces that are configured in this VSAN.

The interface range must be in ascending order and nonoverlapping. You can specify a range using a hyphen and several interfaces using commas:

- The interface range format for a Fibre Channel interface range is fcslot/port - port, fcslot/port, fcslot/port:

  For example, **`show int fc2/1 - 3 , fc2/4 , fc3/2`**

Examples

This example shows how to display the configured VSAN information:

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

switch#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the membership information for all VSANs:

```
switch # show vsan membership
vsan 1 interfaces:

vsan 331 interfaces:
    fc2/3             fc2/4             san-port-channel 14 vfc1
    vfc2              vfc3              vfc4              vfc5
    vfc6              vfc7              vfc8              vfc9
    vfc10             vfc11             vfc12             vfc13
    vfc14             vfc15             vfc16             vfc17
    vfc18             vfc19             vfc20

vsan 332 interfaces:
    fc2/5             fc2/6             fc2/7             fc2/8
    san-port-channel 8 san-port-channel 9 vfc21             vfc22
    vfc23             vfc24             vfc25             vfc26
    vfc27             vfc28             vfc29             vfc30
    vfc31             vfc32             vfc33             vfc34
    vfc35             vfc36             vfc37             vfc38
    vfc39             vfc40

vsan 333 interfaces:
fc2/1             fc2/2             san-port-channel 13

vsan 334 interfaces:

vsan 336 interfaces:

vsan 337 interfaces:

vsan 4079(evfp_isolated_vsan) interfaces:

vsan 4094(isolated_vsan) interfaces:

switch#
```

This example shows how to display the membership information for a specified interface:

```
switch# show vsan membership interface fc2/1
fc2/1
        vsan:333
        allowed list:1-4078,4080-4093
switch#
```

Related Commands

Command	Description
vsan	Configures a VSAN.

Send comments to nx5000-docfeedback@cisco.com

show wwn

To display the status of the WWN configuration, use the **show wwn** command.

show wwn {**status** [**block-id** *number*] | **switch** | **vsan-wwn**}

Syntax Description

status	Displays a summary of the WWN usage and alarm status.
block-id *number*	(Optional) Displays the WWN usage and alarm status for a block ID. The range is from 34 to 1793.
switch	Displays the switch WWN.
vsan-wwn	Displays all user-configured VSAN WWNs.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the WWN of the switch:

```
switch# show wwn switch
```

This example shows how to display a user-configured VSAN WWN:

```
switch# show wwn vsan-wwn
```

Related Commands

Command	Description
wwn vsan	Configures a WWN for a suspended VSAN that has interop mode 4 enabled.

Send comments to nx5000-docfeedback@cisco.com

show zone

To display zone information, use the **show zone** command.

show zone [**active** [**vsan** *vsan-id*] | **analysis** {**active vsan** *vsan-id* | **vsan** *vsan-id* | **zoneset** *zoneset-name*} | **ess** [**vsan** *vsan-id*] | **member** {**fcalias** *alias-name* | **fcid** *fc-id* [**active** | **lun** *lun-id* | **vsan** *vsan-id*] | **pwwn** *wwn* [**active** | **lun** *lun-id* | **vsan** *vsan-id*]} | **name** *string* [**active**] [**pending**] [**vsan** *vsan-id*] | **pending** [**active**] [**vsan** *vsan-id*] | **pending-diff** [**vsan** *vsan-id*] | **policy** [**pending**] [**vsan** *vsan-id*] | **statistics** [**vsan** *vsan-id*] | **status** [**vsan** *vsan-id*]]

Syntax Description

active	(Optional) Displays zones that are part of active zone set.
vsan *vsan-id*	(Optional) Displays zones belonging to the specified VSAN ID. The range is from 1 to 4093.
analysis	(Optional) Displays the analysis of the zone database.
active	Displays the analysis of the active zone database.
vsan	Displays the analysis of the zone database for the specified VSAN.
zoneset *zoneset-name*	Displays the analysis of the specified zone set.
ess	(Optional) Displays the exchange switch support (ESS) information.
member	(Optional) Displays all zones in which the given member is part of.
fcalias *alias-name*	Displays member information for a specific fcalias.
fc-id *fc-id*	Displays member information for a specific Fibre Channel ID.
lun *lun-id*	Displays the logical unit ID.
pwwn *wwwn*	Displays device name information for a specific pWWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
name *string*	Displays members of a specified zone.
pending	Displays members of a specified zone in the current session.
pending-diff	Displays pending changes to the zone database.
statistics	Displays zone server statistics.
status	Displays the zone server current status.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured zone information:

```
switch# show zone
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the zone information for a specific VSAN:

```
switch# show zone vsan 1
```

This example shows how to display the members of a specific zone:

```
switch# show zone name Zone1
```

This example shows how to display all zones to which a member belongs using the FCID:

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
```

This example shows how to display the number of control frames exchanged with other switches:

```
switch# show zone statistics
```

This example shows how to display the status of the configured zones:

```
switch# show zone status
```

This example checks the status of the **zoneset distribute vsan** command and displays the default zone attributes of a specific VSAN or all active VSANs:

```
switch# show zone status vsan 1
VSAN:1 default-zone:deny distribute:active only Interop:default
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases:0
Active Zoning Database :
    Database Not Available
Status:
```

Table 9-3 describes the significant fields shown in the **show zone status vsan** display.

Table 9-3 show zone status Field Descriptions

Field	Description
VSAN:	VSAN number displayed.
default-zone:	Default-zone policy, either permit or deny.
Default zone:	Field that displays the attributes for the specified VSAN. The attributes include Qos level, broadcast zoning enabled/disabled, and read-only zoning enabled/disabled.
distribute:	Distribute full-zone set (full) or active-zone set (active only).
Interop:	Interop mode. 100 = default, 1 = standard, 2 and 3 = Non-Cisco vendors.
mode:	Zoning mode, either basic or enhanced.
merge control:	Merge policy, either allow or restrict.
Hard zoning is enabled	If hardware resources (TCAM) becomes full, hard zoning is automatically disabled.
Full Zoning Database:	Values of zone database.
Active Zoning Database:	Values of active zone database.
Status:	Status of last zone distribution.

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
zone	Configures zone information.

Send comments to nx5000-docfeedback@cisco.com

show zone analysis

To display detailed analysis and statistical information about the zoning database, use the **show zone analysis** command.

show zone analysis {**active vsan** *vsan-id* | **vsan** *vsan-id* | **zoneset** *name* **vsan** *vsan-id*}

Syntax Description

active	Displays analysis information for the active zone set.
vsan *vsan-id*	Displays analysis information for the specified VSAN ID. The range is from 1 to 4093.
zoneset *name*	Displays zone set analysis information for the specified zone set.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the detailed statistics and analysis of the active zoning database:

```
switch# show zone analysis active vsan 1
```

This example shows how to display the detailed statistics and analysis of the full zoning database:

```
switch# sh zone analysis vsan 1
   Zoning database analysis vsan 1
     Full zoning database
       Last updated at: 14:36:56 UTC Oct 04 2005
       Last updated by: Local [CLI / SNMP / GS / CIM / INTERNAL] or
                        Merge [interface] or
                        Remote [Domain, IP-Address]
                               [Switch name]
       Num zonesets: 1
       Num zones: 1
       Num aliases: 0
       Num attribute groups: 0
       Formatted database size: < 1 Kb / 2000 kb ( < 1% usage)

     Unassigned zones:
       zone name z1 vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

Table 9-4 describes the fields displayed in the output of a **show zone analysis** command for the full zoning database.

Table 9-4 show zone analysis Field Descriptions for the Full Zoning Database

Field	Description
Last updated at	Time stamp that shows when the full zoning database was last updated.
Last Updated by	Agent that most recently modified the full zoning database. The agent can be one of the following three types: • Local—Indicates that the full database was last modified locally through a configuration change from one of the following applications: – CLI—The full zoning database was modified by the user from the command line interface. – SNMP—The full zoning database was modified by the user through the Simple Network Management Protocol (SNMP). – GS—The full zoning database was modified from the Generic Services (GS) client. – CIM—The full zoning database was modified by the applications using the Common Information Model (CIM). – INTERNAL—The full zoning database was modified as a result of an internal activation either from Inter-VSAN Routing (IVR) or from the IP storage services manager. • Merge—Indicates that the full database was last modified by the Merge protocol. In this case, the interface on which the merge occurred is also displayed. • Remote—Indicates that the full database was last modified by the Change protocol, initiated by a remote switch, when the full zone set distribution was enabled. The domain, IP address, and switch name of the switch initiating the change are also displayed. **Note** The switch name is displayed on the next line, aligned with the domain, only if the switch name is set. The default switch name *switch* and the *ip-address* are not displayed.
Num zonesets	Total number of zone sets in the database.
Num zones	Total number of zones in the database, including unassigned zones.
Num aliases	Total number of aliases in the database, including unassigned FC aliases.
Num attribute groups	Total number of attribute groups in the database. This field applies only when enhanced zoning is used.

Send comments to nx5000-docfeedback@cisco.com

Table 9-4 show zone analysis Field Descriptions for the Full Zoning Database (continued)

Field	Description
Formatted database size	Total size of the full database when formatted to be sent over the wire. The formatted database size is displayed in kilobytes in this format: < *X* KB / *Y* KB, as in the following example: Formatted database size: < 1 KB/2000 KB In this example, the formatted database size is less than 1 KB out of the maximum size of 2000 KB.
Unassigned zones	All the unassigned zones in the VSAN. Only the names of the zones are displayed. The details about the members of the zone are not displayed in this section.

This example shows how to display the zone set analysis information:

```
switch# show zone analysis zoneset zs1 vsan 1
```

Related Commands

Command	Description
zone compact database	Compacts a zone database in a VSAN.

Send comments to nx5000-docfeedback@cisco.com

show zoneset

To display the configured zone sets, use the **show zoneset** command.

show zoneset [**active** [**vsan** *vsan-id*] | **brief** [**active** [**vsan** *vsan-id*] | **vsan** *vsan-id*] | **name** *zoneset-name* [**active** [**vsan** *vsan-id*] | **brief** [**active** [**vsan** *vsan-id*] | **vsan** *vsan-id*] | **vsan** *vsan-id*] | **pending** [**active** [**vsan** *vsan-id*] | **brief** [**active** [**vsan** *vsan-id*] | **vsan** *vsan-id*] | **vsan** *vsan-id*] | **vsan** *vsan-id*

Syntax Description

active	(Optional) Displays only active zone sets.
vsan *vsan-id*	(Optional) Displays the VSAN. The range is from 1 to 4093.
brief	(Optional) Displays zone set members in a brief list.
name *zoneset-name*	(Optional) Displays members of a specified zone set.
pending	(Optional) Displays zone sets members that are in session.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured zone set information:

```
switch# show zoneset vsan 1
```

This example shows how to display the configured zone set information for a specific VSAN:

```
switch# show zoneset vsan 2-3
```

Related Commands

Command	Description
zoneset (Global configuration mode)	Groups zones under one zone set.
zoneset (EXEC mode)	Merges zone set databases.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 10

vPC Commands

This chapter describes the Cisco NX-OS vPC commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

peer-config-check-bypass

To ignore type checks on the primary vPC device when the multichassis EtherChannel trunk (MCT) is down, use the **peer-config-check-bypass** command. To stop ignoring type checks, use the **no** form of this command.

peer-config-check-bypass

no peer-config-check-bypass

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

vPC domain configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

The peer link, also known as the multichassis EtherChannel trunk (MCT), connects the vPC peer switches. The peer link is always forwarding. The bridge protocol data units (BPDUs) or Link Aggregation Control Protocol (LACP) packets that are received by the secondary vPC peer on a vPC port are forwarded to the primary vPC peer through the peer link for processing.

The peer link is used to synchronize the MAC addresses of the vPC peer switches to provide the necessary transport for multicast traffic. It is also used for forwarding traffic that originates at, or is destined for, orphan ports (that is, a non-vPC port).

Examples

This example shows how to configure the primary vPC device to ignore type checks when the MCT is down:

```
switch(config-vpc-domain)# peer-config-check-bypass
switch(config-vpc-domain)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc brief	Displays brief information about each vPC domain.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show vpc peer-keepalive	Displays the status of the peer-keepalive link.
show vpc statistics	Displays information about the configuration for the keepalive messages.

Send comments to nx5000-docfeedback@cisco.com

peer-keepalive

To configure the IPv4 address for the remote end of the vPC peer keepalive link that carries the keepalive messages, use the **peer-keepalive** command. To disassociate the peer keepalive link, use the **no** form of this command.

peer-keepalive destination *ipv4_address* [**hold-timeout** *holdtime_seconds* | **interval** *mseconds* {**timeout** *seconds*} | {**precedence** {*prec_value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}} | **source** *ipv4_address* | **tos** {*tos_value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte** *tos_byte_value* | **udp-port** *udp_port* | **vrf** {*vrf_name* | **management**}]

no peer-keepalive destination *ipv4_address* [**hold-timeout** *holdtime_seconds* | **interval** *mseconds* {**timeout** *seconds*} | {**precedence** {*prec_value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}} | **source** *ipv4_address* | **tos** {*tos_value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte** *tos_byte_value* | **udp-port** *udp_port* | **vrf** {*vrf_name* | **management**}]

Syntax Description

destination	Specifies the remote (secondary) vPC device interface.
ipv4_address	IPv4 address of the vPC device in the *A.B.C.D* format.
hold-timeout *holdtime_seconds*	(Optional) Specifies the hold-timeout period (in seconds) for the secondary vPC peer device to ignore vPC peer-keepalive messages. The range is from 3 to 10. The default hold-timeout value is 3 seconds.
interval *mseconds*	(Optional) Specifies the time interval (in milliseconds) at which the vPC device receives peer-keepalive messages. The range is from 400 to 10000. The default interval time for the vPC peer-keepalive message is 1 second.
timeout *seconds*	(Optional) Specifies the timeout (in seconds) between retransmissions to the remote (secondary) vPC device. The range is from 3 to 20. The default timeout value is 5 seconds.
precedence	(Optional) Classifies the vPC peer-keepalive interface traffic based on the precedence value in the type of service (ToS) byte field of the IP header. The precedence value can be one of the following: • *prec_value*—IP precedence value. The range is from 0 to 7. The default precedence value is 6. • **critical**—Critical precedence (5) • **flash**—Flash precedence (3) • **flash-override**—Flash-override precedence (4) • **immediate**—Immediate precedence (2) • **internet**—Internet precedence (6) • **network**—Network precedence (7) • **priority**—Priority precedence (1) • **routine**—Routine precedence (0)
source	(Optional) Specifies the source (primary) vPC device interface.

Send comments to nx5000-docfeedback@cisco.com

tos	(Optional) Specifies the type of service (ToS) value. The ToS value can be one of the following: • *tos_value*—A 4-bit TOS value. The range is from 0 to 15. • **max-reliability**—Max-reliability (2) • **max-throughput**—Max-throughput (4) • **min-delay**—Min-delay (8) • **min-monetary-cost**—Min-monetary-cost (1) • **normal**—Normal (0)
tos-byte *tos_byte_value*	(Optional) Specifies a 8-bit TOS value. The range is from 0 to 255.
udp-port *udp_port*	(Optional) Specifies the UDP port number to be used for the peer keepalive link. The range is from 1024 to 65000.
vrf *vrf_name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) name to be used for the peer keepalive link. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
management	Specifies the management VRF. This is the default VRF.

Command Default

Management port and VRF

Command Modes

vPC domain configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

You must configure the vPC peer-keepalive link before the system can form the vPC peer link. Ensure that both the source and destination IP addresses used for the peer-keepalive message are unique in your network and these IP addresses are reachable from the Virtual Routing and Forwarding (VRF) associated with the vPC peer-keepalive link.

The Cisco NX-OS software uses the peer-keepalive link between the vPC peers to transmit periodic, configurable keepalive messages. You must have Layer 3 connectivity between the peer devices to transmit these messages. The system cannot bring up the vPC peer link unless the peer-keepalive link is already up and running.

Note We recommend that you configure a separate VRF instance and put a Layer 3 port from each vPC peer device into that VRF for the vPC peer-keepalive link. Do not use the peer link itself to send vPC peer-keepalive messages.

Examples

This example shows how to set up the peer keepalive link connection between the primary and secondary vPC device:

```
switch(config)# vpc domain 100
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config-vpc-domain)# peer-keepalive destination 192.168.2.2 source 192.168.2.1
Note:
 --------:: Management VRF will be used as the default VRF ::--------
switch(config-vpc-domain)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
vpc peer-link	Creates the vPC peer link between the vPC peer devices.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc peer-keepalive	Displays the status of the peer-keepalive link.
show vpc statistics	Displays information about the configuration for the keepalive messages.

Send comments to nx5000-docfeedback@cisco.com

role

To manually assign a primary or secondary role to a vPC device, use the **role** command. To restore the default role priority, use the **no** form of this command.

role priority *priority_value*

no role priority *priority_value*

Syntax Description

priority	Specifies the priority to define primary or secondary roles in the vPC configuration.
priority_value	Priority value for the vPC device. The range is from 1 to 65535.

Command Default

None

Command Modes

vPC domain configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

By default, the Cisco NX-OS software elects a primary and secondary vPC peer device after you configure the vPC domain and both sides of the vPC peer link. However, you may want to elect a specific vPC peer device as the primary device for the vPC. Then, you would manually configure the role value for the vPC peer device that you want as the primary device to be lower than the other vPC peer device.

vPC does not support role preemption. If the primary vPC peer device fails, the secondary vPC peer device takes over to become operationally the vPC primary device. However, the original operational roles are not restored if the formerly primary vPC comes up again.

Examples

This example shows how to configure the role priority of a vPC device:

```
switch(config-vpc-domain)# role priority 100
switch(config-vpc-domain)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc role	Displays the vPC system priority.

Send comments to nx5000-docfeedback@cisco.com

show feature

To display the status of features on a switch, use the **show feature** command.

show feature

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the state of all features on a switch:

```
switch# show feature
Feature Name          Instance  State
--------------------  --------  --------
cimserver             1         disabled
fabric-binding        1         disabled
fc-port-security      1         disabled
fcoe                  1         enabled
fcsp                  1         disabled
fex                   1         enabled
fport-channel-trunk   1         disabled
http-server           1         enabled
interface-vlan        1         enabled
lacp                  1         enabled
lldp                  1         enabled
npiv                  1         enabled
npv                   1         disabled
port_track            1         disabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
udld                  1         enabled
vpc                   1         enabled
vtp                   1         disabled
switch#
```

Related Commands

Command	Description
feature	Enables or disables a feature on the switch.

Send comments to nx5000-docfeedback@cisco.com

show module

To display module information, use the **show module** command.

show module *module_num*

Syntax Description

module_num	Module number in the switch chassis. The range is from 1 to 3.

Command Default

Display information of all modules

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
switch# show module 1
Mod Ports  Module-Type                      Model                 Status
--- -----  -------------------------------- --------------------- ------------
1    40     40x10GE/Supervisor               N5K-C5020P-BF-SUP      active *

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    4.2(1u)N1(1u)   1.3     --

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    0005.9b78.6e48 to 0005.9b78.6e6f         JAF1413ADCS
switch#
```

Related Commands

Command	Description
show hardware inventory	Displays information about the physical hardware.
show inventory	Displays hardware inventory information.

Send comments to nx5000-docfeedback@cisco.com

show port-channel capacity

To display the number of port channels that are configured, or are still available on the device, use the **show port-channel capacity** command.

show port-channel capacity

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Examples

This example shows how to display the port channels on a device:

```
switch# show port-channel capacity
Port-channel resources
    768 total    120 used    648 free    15% used
switch#
```

Related Commands

Command	Description
show vpc brief	Displays brief information about the vPCs.

Send comments to nx5000-docfeedback@cisco.com

show running-config interface

To display the running configuration for a specific port channel, use the **show running-config interface** command.

show running-config interface [**all** | {**ethernet** {*slot/port*} [**all**]} | **expand-port-profile** | {**loopback** {*number*} [**all**]} | {**mgmt 0** [**all**]} | {**port-channel** {*channel-number*} [**membership**]} | {**tunnel** {*number*} [**all**]} | {**vlan** {*vlan-id*} [**all**]}

Syntax Description

all	(Optional) Displays the configuration with defaults.
ethernet *slot/port*	Displays the Ethernet interface slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
expand-port-profile	Displays the port profiles.
loopback *number*	Displays the number of the loopback interface. The range of values is from 1 to 4096.
mgmt 0	Displays the configuration information of the management interface.
port-channel *channel-number*	Displays the number of the port-channel group. The range of values is from 0 to 1023.
membership	Displays the membership of the specified port channel.
tunnel *number*	Displays the number of the tunnel interface. The range of values is from 0 to 65535.
vlan *vlan-id*	Displays the number of the VLAN. The range of values is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the running configuration for port channel 10:

```
switch(config)# show running-config interface port-channel 10
version 4.0(1)

interface port-channel10
  switchport
  switchport mode trunk

switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show running-config	Displays the running configuration on the device.

Send comments to nx5000-docfeedback@cisco.com

show running-config vpc

To display the running configuration information for virtual port channels (vPCs), use the **show running-config vpc** command.

show running-config vpc [**all**]

Syntax Description

all	(Optional) Displays the running configuration for a vPC with defaults.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the running configuration for a vPC:

```
switch# show running-config vpc

!Command: show running-config vpc
!Time: Wed Mar 31 06:11:52 2010

version 4.2(1)N1(1)
feature vpc

vpc domain 1000
  role priority 2000
  peer-keepalive destination 192.168.183.52 source 192.168.76.51 vrf management
  peer-config-check-bypass


interface port-channel1
  vpc peer-link

interface port-channel3
  vpc 4096

interface port-channel5
  vpc 4001

interface port-channel12
  vpc 4000

interface port-channel24
  vpc 2000

interface port-channel41
  vpc 41
```

Send comments to nx5000-docfeedback@cisco.com

```
interface port-channel48
  vpc 48

--More--
switch#
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, this command returns an error.

Send comments to nx5000-docfeedback@cisco.com

show startup-config interface

To display interface configuration information in the startup configuration, use the **show startup-config interface** command.

show startup-config interface [**ethernet** *slot/port* | **expand-port-profile** | **loopback** *number* | **mgmt 0** | **port-channel** {*channel-number*} [**membership**] | **tunnel** *number* | {**vlan** *vlan-id*}

Syntax Description

ethernet *slot/port*	(Optional) Displays the number of the module and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
expand-port-profile	Displays the port profiles.
loopback *number*	Displays the number of the loopback interface. The range of values is from 1 to 4096.
mgmt 0	Displays the configuration information of the management interface.
port-channel *channel-number*	Displays the number of the port-channel group. The range of values is from 0 to 1023.
membership	(Optional) Displays the membership of the specified port channel.
tunnel *number*	Displays the number of the tunnel interface. The range of values is from 0 to 65535.
vlan *vlan-id*	Displays the number of the VLAN. The range of values is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the information in the startup configuration for the interface Ethernet 7/1:

```
switch(config)# show startup-config interface ethernet 7/1
version 4.1(2)

interface Ethernet7/1
  ip pim sparse-mode
switch(config)#
```

Related Commands

Command	Description
show interface	Displays information about the specified interface.

Send comments to nx5000-docfeedback@cisco.com

show startup-config vpc

To display virtual port channel (vPC) configuration information in the startup configuration, use the **show startup-config vpc** command.

show startup-config vpc [**all**]

Syntax Description[

all	(Optional) Displays startup-configuration information for all vPCs.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the vPC information in the startup configuration:

```
switch(config)# show startup-config vpc
version 4.1(2)
feature vpc
vpc domain 1


interface port-channel10
  vpc peer-link

interface port-channel20
  vpc 100
switch(config)#
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

Send comments to nx5000-docfeedback@cisco.com

show tech-support vpc

To display troubleshooting information about the virtual port channel (vPC), use the **show tech-support vpc** command.

show tech-support vpc

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Examples

This example shows how to display the vPC troubleshooting information:

```
switch# show tech-support vpc
`show version`
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2010, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.3.0
  loader:    version N/A
  kickstart: version 4.2(1)N1(1) [build 4.2(1)N1(0.329)]
  system:    version 4.2(1)N1(1) [build 4.2(1)N1(0.329)]
  power-seq: version v1.2
  BIOS compile time:       09/08/09
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.2.1.N1.latest.bin
  kickstart compile time:  4/18/2010 8:00:00 [04/18/2010 15:03:44]
  system image file is:    bootflash:/n5000-uk9.4.2.1.N1.latest.bin
  system compile time:     4/18/2010 8:00:00 [04/18/2010 16:08:18]


Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU    with 2074284 kB of memory.
  Processor Board ID JAF1413ADCS

  Device name: d14-switch-2
  bootflash:    1003520 kB

Kernel uptime is 0 day(s), 2 hour(s), 25 minute(s), 26 second(s)
```

Send comments to nx5000-docfeedback@cisco.com

```
Last reset at 414529 usecs after  Mon Apr 19 05:59:19 2010

  Reason: Disruptive upgrade
  System version: 4.2(1u)N1(1u)
  Service:

plugin
  Core Plugin, Ethernet Plugin, Fc Plugin
`show module`
Mod Ports  Module-Type                       Model                  Status
--- -----  ------------------------------- ---------------------- ------------
1    40     40x10GE/Supervisor              N5K-C5020P-BF-SUP      active *
2    8      8x1/2/4G FC Module              N5K-M1008              ok
3    6      6x10GE Ethernet Module          N5K-M1600              ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    4.2(1)N1(1)     1.3     --
2    4.2(1)N1(1)     0.200   20:41:00:05:9b:78:6e:40 to 20:48:00:05:9b:78:6e:40
3    4.2(1)N1(1)     0.100   --

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    0005.9b78.6e48 to 0005.9b78.6e6f         JAF1413ADCS
2    0005.9b78.6e70 to 0005.9b78.6e77         JAB1228016M
3    0005.9b78.6e78 to 0005.9b78.6e7f         JAB12310214
`show vpc brief`
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 1000
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
vPC role                          : secondary
Number of vPCs configured         : 150
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-330,335,338-447,1000-1023,2000-2018

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
41     Po41        down*  failed      Consistency Check Not      -
                                      Performed
48     Po48        down*  failed      Consistency Check Not      -
                                      Performed
2000   Po24        down   success     success                    -
4000   Po12        down   success     success                    -
4001   Po5         down   success     success                    -
4096   Po3         down   success     success                    -
101376 Eth100/1/1  down*  failed      Consistency Check Not      -
                                      Performed
101377 Eth100/1/2  down*  failed      Consistency Check Not      -
                                      Performed
101378 Eth100/1/3  down*  failed      Consistency Check Not      -
                                      Performed
```

Send comments to nx5000-docfeedback@cisco.com

```
101379 Eth100/1/4  down*  failed      Consistency Check Not      -
                                      Performed
101380 Eth100/1/5  down*  failed      Consistency Check Not      -
--More--
switch#
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

Send comments to nx5000-docfeedback@cisco.com

show vpc

To display detailed information about the virtual port channels (vPCs) configured on the switch, use the **show vpc** command.

show vpc [*vpc-number*]

Syntax Description

vpc-number	(Optional) vPC number. The range is from 1 to 4096.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Examples

This example shows how to display the vPC information:

```
switch# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Type-2 consistency reason         : Consistency Check Not Performed
vPC role                          : secondary
Number of vPCs configured         : 1
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po4000 up     1,3001-3500

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
10     Po10        up     success     success                    3001-3200

switch#
```

This example shows how to display information about a specific vPC:

```
switch# show vpc 10
```

Send comments to nx5000-docfeedback@cisco.com

```
vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
10     Po10        up     success     success                    3001-3200

switch#
```

Related Commands

Command	Description
show vpc brief	Displays vPC information in a brief summary.
vpc	Configures vPC features on the switch.

Send comments to nx5000-docfeedback@cisco.com

show vpc brief

To display brief information about the virtual port channels (vPCs), use the **show vpc brief** command.

show vpc brief [**vpc** *number*]

Syntax Description

vpc *number*	(Optional) Displays the brief information for the specified vPC. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The **show vpc brief** command displays the vPC domain ID, the peer-link status, the keepalive message status, whether the configuration consistency is successful, and whether a peer link formed or failed to form.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information about enabling vPCs.

You can display the track object if you have configured a tracked object for running vPCs on a single module in the vpc-domain configuration mode.

Examples

This example shows how to display brief information about the vPCs:

```
switch(config)# show vpc brief

Legend:
                (*) - local vpc is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
vPC role                          : primary
Number of vPC configured          : 1

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10   up     1-100

vPC status
----------------------------------------------------------------------
```

Send comments to nx5000-docfeedback@cisco.com

```
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- -------------------------- ------------
20   Po20   up     success     success                    1-100
switch(config)#
```

This example shows how to display brief information about the vPCs. In this example, the port channel failed the consistency check, and the device displays the reason for the failure:

```
switch(config)# show vpc brief

Legend:
                (*) - local vpc is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: failed
Configuration consistency reason: vPC type-1 configuration incompatible - STP interface
port type inconsistent
vPC role                          : secondary
Number of vPC configured          : 1

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10   up     1-100

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- -------------------------- ------------
20   Po20   up     failed      vPC type-1 configuration   -
                                incompatible - STP
                                interface port type
                                inconsistent
switch(config)#
```

This example shows how to display information about the tracked objects in the vPCs:

```
switch(config)# show vpc brief

Legend:
                (*) - local vpc is down, forwarding via vPC peer-link

vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
vPC role                          : secondary
Number of vPC configured          : 3
Track object                      : 12


vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10   up     1-100
switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
feature vpc	Enables vPCs on the device.
show port channel summary	Displays information about port channels.
vpc	Configures vPC domains and peers.

Send comments to nx5000-docfeedback@cisco.com

show vpc consistency-parameters

To display the consistency of parameters that must be compatible across the virtual port-channel (vPC) interfaces, use the **show vpc consistency-parameters** command.

show vpc consistency-parameters {**global** | **interface port-channel** *channel-number* | **vpc** *number*}

Syntax Description

global	(Optional) Displays the configuration of all Type 1 global parameters on both sides of the vPC peer link.
interface port-channel *channel-number*	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link.
vpc *number*	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link for the specified vPC.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The **show vpc consistency-parameters** command displays the configuration of all the vPC Type 1 parameters on both sides of the vPC peer link.

Note All the Type 1 configurations must be identical on both sides of the vPC peer link, or the link will not come up.

The vPC Type 1 configuration parameters are as follows:

- Port-channel mode: on, off, or active
- Link speed per channel
- Duplex mode per channel
- Trunk mode per channel
  - Native VLAN
  - VLANs allowed on trunk
  - Tagging of native VLAN traffic
- Spanning Tree Protocol (STP) mode
- STP region configuration for Multiple Spanning Tree

Send comments to nx5000-docfeedback@cisco.com

- Enable/disable state the same per VLAN
- STP global settings
  - Bridge Assurance setting
  - Port type setting—We recommend that you set all vPC peer link ports as network ports.
  - Loop Guard settings
- STP interface settings:
  - Port type setting
  - Loop Guard
  - Root Guard
- Maximum transmission unit (MTU)
- Allowed VLAN bit set

This command is not available if you have not enabled the vPC feature. See **feature vpc** for information on enabling vPCs.

Examples

This example shows how to display the vPC consistency parameters for the specified port channel:

```
switch(config)# show vpc consistency-parameters global

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
QoS                         1     ([], [3], [0], [1-2],  ([], [3], [0], [1-2],
                                  [4-5], [6])            [4-5], [6])
Network QoS (MTU)           1     (1538, 2240, 5038,     (1538, 2240, 5038,
                                  4038, 9216, 9216)      4038, 9216, 9216)
Network Qos (Pause)         1     (F, T, F, F, F, F)     (F, T, F, F, F, F)
Input Queuing (Bandwidth)   1     (5, 10, 20, 0, 20, 40) (5, 10, 20, 0, 20, 40)
Input Queuing (Absolute     1     (F, F, F, T, F, F)     (F, F, F, T, F, F)
Priority)
Output Queuing (Bandwidth)  1     (5, 10, 20, 0, 20, 40) (5, 10, 20, 0, 20, 40)
Output Queuing (Absolute    1     (F, F, F, T, F, F)     (F, F, F, T, F, F)
Priority)
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
 VLAN Mapping
STP Loopguard               1     Disabled               Disabled
STP Bridge Assurance        1     Enabled                Enabled
STP Port Type, Edge         1     Normal, Disabled,      Normal, Disabled,
BPDUFilter, Edge BPDUGuard        Disabled               Disabled
STP MST Simulate PVST       1     Enabled                Enabled
Allowed VLANs               -     1-330,335,338-450,1000 1-330,333-447,1000-102
                                  -1023,2000-2023        8,2000-2018
Local suspended VLANs       -     331-334,336-337,448-45 -
                                  0,2019-2023

switch(config)#
```

This example shows how to display the vPC consistency parameters for the specified port channel:

```
switch(config)# show vpc consistency-parameters interface port-channel 20
```

Send comments to nx5000-docfeedback@cisco.com

```
Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name            Type Local Value              Peer Value
-------------   ---- ---------------------- -------------------------
STP Port Type   1    Default                  Default
STP Port        1    None                     None
Guard
mode            1    on                       on
Speed           1    10 Gb/s                  10 Gb/s
Duplex          1    full                     full
Port Mode       1    trunk                    trunk
Native Vlan     1    1                        1
MTU             1    1500                     1500
Allowed VLAN    -    1-100                    1-100
bitset
switch(config)#
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
show port channel summary	Displays information about port channels.
vpc	Configures vPC domains and peers.

Send comments to nx5000-docfeedback@cisco.com

show vpc orphan-ports

To display ports that are not part of the virtual port channel (vPC) but have common VLANs, use the **show vpc orphan-ports** command.

show vpc orphan-ports

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The **show vpc orphan-ports** command displays those ports that are not part of the vPC but that share common VLANs with ports that are part of the vPC.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information about enabling vPCs.

Examples

This example shows how to display vPC orphan ports:

```
switch(config)# show vpc orphan-ports

Note:
--------::Going through port database. Please be patient.::--------

VLAN            Orphan Ports
-------         -------------------------
1               Po600
2               Po600
3               Po600
4               Po600
5               Po600
6               Po600
7               Po600
8               Po600
9               Po600
10              Po600
11              Po600
12              Po600
13              Po600
14              Po600
--More--
switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
feature vpc	Enables vPCs on the device.
show vpc brief	Displays brief information about vPCs.

Send comments to nx5000-docfeedback@cisco.com

show vpc peer-keepalive

To display the destination IP for the virtual port-channel (vPC) peer keepalive message and the status of the messages, use the **show vpc peer-keepalive** command.

show vpc peer-keepalive

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The show **vpc peer-keepalive** command displays the destination IP of the peer keepalive message for the vPC. The command also displays the send and receive status as well as the last update from the peer in seconds and milliseconds.

Note We recommend that you create a separate VRF on the peer devices to send and receive the vPC peer keepalive messages. Do not use the peer link itself to send the vPC peer-keepalive messages.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information about enabling vPCs.

Examples

This example shows how to display information about the peer-keepalive message:

```
switch(config)# show vpc peer-keepalive

vPC keep-alive status           : peer is alive
--Send status                   : Success
--Last send at                  : 2008.05.17 18:23:53 986 ms
--Sent on interface             : Eth7/16
--Receive status                : Success
--Last receive at               : 2008.05.17 18:23:54 99 ms
--Received on interface         : Eth7/16
--Last update from peer         : (0) seconds, (486) msec

vPC Keep-alive parameters
--Destination                   : 192.168.145.213
--Keepalive interval            : 1000 msec
--Keepalive timeout             : 5 seconds
--Keepalive hold timeout        : 3 seconds
--Keepalive vrf                 : pkal
--Keepalive udp port            : 3200
```

Send comments to nx5000-docfeedback@cisco.com

```
--Keepalive tos                : 192
switch(config)#
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

Send comments to nx5000-docfeedback@cisco.com

show vpc role

To display information about the virtual port-channel (vPC) role of the peer device, use the **show vpc role** command.

show vpc role

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The **show vpc role** command displays the following information about the vPC status:

- Status of peer adjacency
- vPC role of the VDC that you are working on
- vPC MAC address
- vPC system priority
- MAC address of the device that you are working on
- System priority for the device that you are working on

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

Examples

This example shows how to display the vPC role information of the device that you are working on:

```
switch(config)# show vpc role

Primary:

vPC Role status
----------------------------------------------------
vPC role                        : primary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:01
vPC system-priority             : 32667
vPC local system-mac            : 00:22:55:79:ea:c1
vPC local role-priority         : 32667


Secondary:
```

Send comments to nx5000-docfeedback@cisco.com

```
vPC Role status
----------------------------------------------------
vPC role                        : secondary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:01
vPC system-priority             : 32667
vPC local system-mac            : 00:22:55:79:de:41
vPC local role-priority         : 32667
switch(config)#
```

When you reload the primary vPC peer device, the secondary vPC peer device assumes the role of the primary device. This example shows how the vPC role displays then on the new primary device:

```
switch(config)# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : secondary, operational primary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:64
vPC system-priority             : 32667
vPC local system-mac            : 00:22:55:79:de:41
vPC local role-priority         : 32667

switch(config)#
```

Related Commands

Command	Description
role	Assigns a primary or secondary role to a vPC device.
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
show port channel summary	Displays information about port channels.

Send comments to nx5000-docfeedback@cisco.com

show vpc statistics

To display virtual port-channel (vPC) statistics, use the **show vpc statistics** command.

show vpc statistics {**peer-keepalive** | **peer-link** | **vpc** *number*}

Syntax Description

peer-keepalive	Displays statistics about the peer-keepalive message.
peer-link	Displays statistics about the peer link.
vpc *number*	Displays statistics about the specified vPC. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)N1(1)	This command was introduced.

Usage Guidelines

The **peer-link** parameter displays the same information as the **show interface port-channel** *channel number* command for the vPC peer-link port channel.

The **vpc** *number* parameter displays the same information as the **show interface port-channel** *channel number* command for the specified vPC port channel.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

Examples

This example shows how to display statistics about the peer-keepalive message:

```
switch# show vpc statistics peer-keepalive

vPC keep-alive status           : peer is alive

VPC keep-alive statistics
--------------------------------------------------
peer-keepalive tx count:          1036
peer-keepalive rx count:          1028
average interval for peer rx:     995
Count of peer state changes:      1
switch(config)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
show port channel summary	Displays information about port channels.

Send comments to nx5000-docfeedback@cisco.com

system-mac

To manually configure the virtual port channel (vPC) domain MAC address, use the **system-mac** command. To restore the default vPC system MAC address, use the **no** form of this command.

system-mac *mac_address*

no system-mac *mac_address*

Syntax Description

mac_address	MAC address that you want for the specified vPC domain in the following format aaaa.bbbb.cccc.

Command Default

None

Command Modes

vPC domain configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

When you create a vPC domain, the Cisco NX-OS software automatically creates a vPC system MAC address, which is used for operations that are confined to the link-scope, such as the Link Aggregation Control Protocol (LACP). However, you may choose to configure the vPC domain MAC address manually.

Examples

This example shows how to configure the MAC address for the vPC domain:

```
switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e
switch(config-vpc-domain)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show vpc peer-keepalive	Displays the status of the peer-keepalive link.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc role	Displays the vPC system priority.
show vpc statistics	Displays information about the configuration for the keepalive messages.

Send comments to nx5000-docfeedback@cisco.com

system-priority

To manually configure a system priority for the virtual port channel (vPC) domain, use the **system-priority** command. To restore the default system priority, use the **no** form of this command.

system-priority *priority_value*

no system-priority *priority_value*

Syntax Description

priority_value	System priority that you want for the specified vPC domain. The range is from 1 to 65535, and the default value is 32667.

Command Default

The default for the system priority is 32667.

Command Modes

vPC domain configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

We recommend that you manually configure the vPC system priority when you are running Link Aggregation Control Protocol (LACP) to ensure that the vPC peer devices are the primary devices on LACP. When you manually configure the system priority, ensure that you configure the same priority value on both vPC peer devices. If these values do not match, vPC will not come up.

Examples

This example shows how to configure the system priority for the vPC domain:

```
switch(config-vpc-domain)# system-priority 3000
switch(config-vpc-domain)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc role	Displays the vPC system priority.

Send comments to nx5000-docfeedback@cisco.com

vpc

To move other port channels into a virtual port channel (vPC) to connect to the downstream device, use the **vpc** command. To remove the port channels from the vPC, use the **no** form of this command.

vpc *number*

no vpc *number*

Syntax Description

number	Port channel number to connect to the downstream device. The range is from 1 and 4096. **Note** The vPC number that you assign to the port channel that connects to the downstream device from the vPC peer device must be identical on both vPC peer devices.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

You can use any module in the device for the port channels.

Note We recommend that you attach the vPC domain downstream port channel to two devices for redundancy.

To connect to the downstream device, you create a port channel from the downstream device to the primary vPC peer device, and you create another port channel from the downstream device to the secondary peer device. Finally, working on each vPC peer device, you assign a vPC number to the port channel that connects to the downstream device. You will experience minimal traffic disruption when you are creating vPCs.

Note The port channel number and vPC number can be different, but the vPC number must be the same on both Cisco Nexus 5000 Series switches.

Examples

This example shows how to configure the selected port channel into the vPC to connect to the downstream device:

```
switch(config)# interface port-channel 20
switch(config-if)# vpc 5
switch(config-if)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc brief	Displays information about each vPC, including information about the vPC peer link.
show vpc consistency-parameters	Displays the status of those parameters that must be consistent across all vPC interfaces.

Send comments to nx5000-docfeedback@cisco.com

vpc domain

To create a virtual port channel (vPC) domain and assign a domain ID, use the **vpc domain** command. To revert to the default vPC configuration, use the **no** form of this command.

vpc domain *domain_id*

no vpc domain *domain_id*

Syntax Description

domain_id	vPC domain ID. The range is from 1 to 1000.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

Before you can create a vPC domain and configure vPC on the switch, you must enable the vPC feature using the **feature vpc** command.

The vPC domain includes both vPC peer devices, the vPC peer keepalive link, the vPC peer link, and all the port channels in the vPC domain connected to the downstream device. You can have only one vPC domain ID on each device.

When configuring the vPC domain ID, make sure that the ID is different from the ID used by a neighboring vPC-capable device with which you may configure a double-sided vPC. This unique ID is needed because the system ID is derived from the MAC address ID of the switch. For a vPC, this MAC address is derived from the domain ID. As a result, in a peer-to-peer vPC configuration, if the neighboring switches use the same domain ID, a system ID conflict may occur in the LACP negotiation that may cause an unsuccessful LACP negotiation.

Under the vPC domain, make sure to configure the primary vPC device to ignore type checks by using the **peer-config-check-bypass** command.

Examples

This example shows how to create a vPC domain:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
feature vpc	Enables or disables a vPC on the switch.
peer-config-check-bypass	Ignores type checks on primary when the MCT is down.
peer-keepalive	Configures the vPC peer keepalive link.
role priority	Configures the role priority for the vPC device.
show vpc brief	Displays brief information about each vPC domain.

Send comments to nx5000-docfeedback@cisco.com

vpc peer-link

To create a virtual port channel (vPC) peer link by designating the port channel that you want on each device as the peer link for the specified vPC domain, use the **vpc peer-link** command. To remove the peer link, use the **no** form of this command.

vpc peer-link

no vpc peer-link

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)N1(1)	This command was introduced.

Usage Guidelines

We recommend that you configure the Layer 2 port channels that you are designating as the vPC peer link in trunk mode and that you use two ports on separate modules on each vPC peer device for redundancy.

The Cisco Nexus 5000 Series switch supports 768 hardware port channels. Use the **show port-channel capacity** command to display the total number of port channels supported by the hardware.

Examples

This example shows how to select the port channel that you want to use as the vPC peer link for this device and configure the selected port channel as the vPC peer link:

```
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
switch(config-vpc-domain)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show port-channel capacity	Reports the number of port channels that are configured and the number of port channels that are still available on the device.
show running-config vpc	Displays the running configuration information for vPCs.
show vpc brief	Displays a brief information about the vPCs.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show vpc brief	Displays information about each vPC, including information about the vPC peer link.
show vpc peer-keepalive	Displays information on the peer-keepalive messages.

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

INDEX

A

B

C

Send comments to nx5000-docfeedback@cisco.com

D

E

F

Send comments to nx5000-docfeedback@cisco.com

G

H

I

Send comments to nx5000-docfeedback@cisco.com

L

M

N

Send comments to nx5000-docfeedback@cisco.com

P

Q

R

S

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

Send comments to nx5000-docfeedback@cisco.com

T

U

Send comments to nx5000-docfeedback@cisco.com

V

W

Z