Send comments to nx5000-docfeedback@cisco.com

Cisco Nexus 5000 Series Command Reference, Release 4.0

October 16, 2008

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-16599-01

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 Command Reference, Release 4.0
© 2008 Cisco Systems, Inc. All rights reserved.

Send comments to nx5000-docfeedback@cisco.com

CONTENTS

Preface xvii

Audience xvii

Organization xvii

Document Conventions xviii

Related Documentation xviii

Obtaining Documentation and Submitting a Service Request xix

Cisco Nexus 5000 Series Basic System Commands 1-1

banner motd 1-2

boot 1-3

cd 1-5

clear cli history 1-6

clear cores 1-7

clear debug-logfile 1-8

clear install failure-reason 1-9

clear license 1-10

clear user 1-11

cli var name 1-12

clock set 1-14

clock summer-time 1-15

clock timezone 1-17

configure terminal 1-18

copy 1-19

copy running-config startup-config 1-23

databits 1-24

debug logfile 1-25

debug logging 1-26

delete 1-27

dir 1-28

echo 1-30

end 1-31

exec-timeout 1-32

Send comments to nx5000-docfeedback@cisco.com

exit (EXEC) 1-34
exit (global) 1-35
feature lldp 1-36
find 1-37
format 1-38
gunzip 1-39
gzip 1-40
hostname 1-41
install all 1-42
install license 1-45
line console 1-46
line vty 1-47
modem in 1-48
modem init-string 1-49
modem set-string user-input 1-51
move 1-52
parity 1-54
ping 1-55
reload 1-57
rmdir 1-58
run-script 1-59
send 1-60
setup 1-61
session-limit 1-62
show banner motd 1-63
show boot 1-64
show cli alias 1-65
show cli history 1-66
show cli variables 1-67
show clock 1-68
show copyright 1-69
show debug logfile 1-70
show environment 1-71
show file 1-72
show hardware internal 1-73

Send comments to nx5000-docfeedback@cisco.com

show hostname 1-74
show incompatibility system 1-75
show install all 1-76
show inventory 1-77
show license 1-78
show license host-id 1-79
show license usage 1-80
show line 1-81
show module 1-82
show processes 1-83
show processes cpu 1-84
show processes log 1-85
show processes memory 1-86
show running-config 1-87
show running-config diff 1-88
show sprom 1-90
show startup-config 1-91
show switchname 1-92
show system cores 1-93
show system reset-reason 1-94
show system uptime 1-95
show tech-support 1-96
show terminal 1-97
show version 1-98
sleep 1-99
speed 1-100
stopbits 1-101
system cores 1-102
system startup-config unlock 1-103
switchname 1-104
tail 1-105
terminal length 1-107
terminal session-timeout 1-108
terminal terminal-type 1-109
terminal width 1-110

Send comments to nx5000-docfeedback@cisco.com

traceroute 1-111
update license 1-112
write erase 1-113

CHAPTER 2 Cisco Nexus 5000 Series Ethernet Commands 2-1

channel-group (Ethernet configuration) 2-2
clear mac access-list counters 2-5
clear mac dynamic 2-6
clear mac-address-table dynamic 2-8
clear ntp session 2-10
clear ntp statistics 2-11
clear spanning-tree counters 2-12
clear spanning-tree detected-protocol 2-13
feature interface-vlan 2-14
feature lacp 2-15
feature private-vlan 2-16
instance vlan 2-17
interface ethernet 2-19
interface port-channel 2-20
interface vethernet 2-22
ip igmp snooping (EXEC) 2-23
ip igmp snooping (VLAN) 2-24
lacp port-priority 2-26
lacp system-priority 2-27
mac-address-table aging-time 2-28
mac-address-table notification 2-30
mac-address-table static 2-31
monitor session 2-33
name (VLAN configuration) 2-34
name (MST configuration) 2-35
ntp 2-36
ntp abort 2-37
ntp commit 2-38
ntp distribute 2-39
ntp sync-retry 2-40
port-channel load-balance ethernet 2-41

Send comments to nx5000-docfeedback@cisco.com

private-vlan 2-43
private-vlan association 2-45
private-vlan synchronize 2-47
revision 2-48
shutdown (VLAN configuration) 2-49
spanning-tree bpdufilter 2-51
spanning-tree bpduguard 2-53
spanning-tree cost 2-55
spanning-tree guard 2-57
spanning-tree link-type 2-58
spanning-tree loopguard default 2-59
spanning-tree mode 2-60
spanning-tree mst configuration 2-61
spanning-tree mst cost 2-63
spanning-tree mst forward-time 2-65
spanning-tree mst hello-time 2-66
spanning-tree mst max-age 2-67
spanning-tree mst max-hops 2-68
spanning-tree mst port-priority 2-69
spanning-tree mst priority 2-70
spanning-tree mst root 2-71
spanning-tree mst simulate pvst 2-73
spanning-tree mst simulate pvst global 2-75
spanning-tree pathcost method 2-77
spanning-tree port type edge 2-78
spanning-tree port type edge bpdufilter default 2-80
spanning-tree port type edge bpduguard default 2-82
spanning-tree port type edge default 2-84
spanning-tree port type network 2-86
spanning-tree port type network default 2-88
spanning-tree port-priority 2-90
spanning-tree vlan 2-91
state 2-93
svi enable 2-94
switchport access vlan 2-95

Send comments to nx5000-docfeedback@cisco.com

switchport block 2-96
switchport mode private-vlan host 2-97
switchport mode private-vlan promiscuous 2-98
switchport private-vlan host-association 2-99
switchport private-vlan mapping 2-101
vlan (EXEC mode) 2-103
vrf context 2-105

CHAPTER 3 Cisco Nexus 5000 Series Ethernet Show Commands 3-1
show interface mac-address 3-2
show interface port-channel 3-3
show interface private-vlan mapping 3-4
show interface switchport 3-5
show interface vlan 3-6
show ip igmp snooping 3-8
show lacp 3-9
show mac-address-table aging-time 3-10
show mac-address-table count 3-11
show mac-address-table notification 3-12
show mac-address-table 3-13
show monitor session 3-15
show port-channel capacity 3-16
show port-channel compatibility-parameters 3-17
show port-channel database 3-18
show port-channel load-balance 3-19
show port-channel summary 3-21
show port-channel traffic 3-22
show port-channel usage 3-23
show running-config 3-24
show running-config spanning-tree 3-25
show running-config vlan 3-26
show spanning-tree 3-27
show spanning-tree active 3-30
show spanning-tree bridge 3-32
show spanning-tree brief 3-34
show spanning-tree detail 3-36

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree interface 3-38
show spanning-tree mst 3-40
show spanning-tree root 3-42
show spanning-tree summary 3-44
show spanning-tree vlan 3-46
show startup-config 3-49
show vlan 3-50
show vlan id 3-52
show vlan private-vlan 3-53

CHAPTER 4 Cisco Nexus 5000 Series Quality of Service Commands 4-1
class-map 4-2
match cos 4-3
policy-map 4-4
service-policy 4-6
system jumbomtu 4-8
system qos 4-9
priority-flow-control 4-10
show class-map 4-11
show policy-map 4-12
show system qos 4-13
show interface priority-flow-control 4-14
show policy-map interface 4-15

CHAPTER 5 Cisco Nexus 5000 Series Security Commands 5-1
aaa accounting default 5-2
aaa authentication login console 5-3
aaa authentication login default 5-5
aaa authentication login error-enable 5-7
aaa authentication login mschap enable 5-8
aaa group server radius 5-9
action 5-10
clear access-list counters 5-11
clear accounting log 5-12
deadtime 5-13
deny (IPv4) 5-15

Send comments to nx5000-docfeedback@cisco.com

deny (MAC) 5-25
description (user role) 5-28
feature 5-29
feature tacacs+ 5-30
interface policy deny 5-31
ip access-list 5-32
ip port access-group 5-34
mac access-list 5-36
mac port access-group 5-38
match 5-40
permit (IPv4) 5-41
permit (MAC) 5-51
permit interface 5-54
permit vlan 5-56
permit vrf 5-58
radius-server deadtime 5-59
radius-server directed-request 5-60
radius-server host 5-61
radius-server key 5-63
radius-server retransmit 5-64
radius-server timeout 5-65
remark 5-66
resequence 5-68
role feature-group name 5-70
role name 5-71
rule 5-72
server 5-74
show aaa accounting 5-76
show aaa authentication 5-77
show aaa groups 5-78
show access-lists 5-79
show accounting log 5-80
show ip access-lists 5-82
show mac access-lists 5-83
show radius-server 5-84

Send comments to nx5000-docfeedback@cisco.com

show role 5-86
show role feature 5-87
show role feature-group 5-88
show running-config aaa 5-89
show running-config radius 5-90
show running-config security 5-91
show ssh key 5-92
show ssh server 5-93
show startup-config aaa 5-94
show startup-config radius 5-95
show startup-config security 5-96
show tacacs-server 5-97
show telnet server 5-99
show user-account 5-100
show users 5-101
show vlan access-list 5-102
show vlan access-map 5-103
show vlan filter 5-104
ssh 5-105
ssh key 5-106
ssh server enable 5-108
storm-control level 5-109
tacacs-server deadtime 5-111
tacacs-server directed-request 5-112
tacacs-server host 5-113
tacacs-server key 5-115
tacacs-server timeout 5-116
telnet 5-117
telnet server enable 5-118
use-vrf 5-119
username 5-121
vlan access-map 5-123
vlan filter 5-124
vlan policy deny 5-126
vrf policy deny 5-127

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 6 Cisco Nexus 5000 Series System Management Commands 6-1

clear logging nvram 6-2
clear logging onboard 6-3
clear logging session 6-4
logging console 6-5
logging level 6-7
logging logfile 6-9
logging module 6-11
logging monitor 6-13
logging server 6-15
logging timestamp 6-17
show logging console 6-18
show logging info 6-19
show logging last 6-20
show logging level 6-21
show logging logfile 6-22
show logging module 6-23
show logging monitor 6-24
show logging nvram 6-25
show logging onboard 6-26
show logging server 6-31
show logging session status 6-32
show logging status 6-33
show logging timestamp 6-34
System Message Logging Facilities 6-35

CHAPTER 7 Cisco Nexus 5000 Series Fibre Channel Commands 7-1

cfs distribute 7-2
cfs ipv4 distribute 7-3
cfs ipv4 mcast-address 7-5
cfs ipv6 distribute 7-7
cfs ipv6 mcast-address 7-9
cfs region 7-11
cfs staggered-merge 7-13
clear device-alias 7-14

Send comments to nx5000-docfeedback@cisco.com

clear fcdomain 7-15
clear fcflow stats 7-16
clear fcns statistics 7-17
clear fcsm log 7-18
clear fcs statistics 7-19
clear fctimer session 7-20
clear fspf counters 7-21
clear port-security 7-22
clear rlir 7-23
clear rscn session 7-24
clear rscn statistics 7-25
clear zone 7-26
device-alias abort 7-27
device-alias commit 7-28
device-alias database 7-29
device-alias distribute 7-30
device-alias import fcalias 7-31
device-alias mode 7-32
device-alias name 7-33
device-alias rename 7-34
discover custom-list 7-35
discover scsi-target 7-36
fabric profile 7-38
fabric-binding activate 7-39
fabric-binding database copy 7-40
fabric-binding database diff 7-41
fabric-binding database vsan 7-42
fabric-binding enable 7-44
fcalias clone 7-45
fcalias name 7-46
fcalias rename 7-47
fcdomain 7-48
fcdomain abort vsan 7-50
fcdomain commit vsan 7-51
fcdomain distribute 7-52

Send comments to nx5000-docfeedback@cisco.com

fcdomain rcf-reject 7-53
fcdroplatency 7-54
fcflow stats 7-55
fcid-allocation 7-57
fcinterop fcid-allocation 7-58
fcns no-auto-poll 7-59
fcns proxy-port 7-60
fcns reject-duplicate-pwwn vsan 7-61
fcping 7-62
fcroute 7-64
fcs plat-check-global 7-66
fcs register 7-67
fcs virtual-device-add 7-68
fcsp 7-69
fcsp dhchap 7-71
fcsp enable 7-73
fcsp reauthenticate 7-74
fcsp timeout 7-75
fctimer 7-76
fctimer abort 7-77
fctimer commit 7-78
fctimer distribute 7-79
fctrace 7-80
fdmi suppress-updates 7-81
feature fcoe 7-82
fspf config 7-83
fspf cost 7-85
fspf dead-interval 7-86
fspf enable 7-87
fspf hello-interval 7-88
fspf passive 7-89
fspf retransmit-interval 7-90
in-order-guarantee 7-91
interface fc 7-92
interface san-port-channel 7-94

Send comments to nx5000-docfeedback@cisco.com

interface vig 7-96
interface vfc 7-97
lldp 7-99
lldp (interface) 7-101
logging abort 7-102
logging commit 7-103
logging distribute 7-104
member (fcalias configuration submode) 7-105
member (zone configuration submode) 7-107
member (zoneset configuration submode) 7-109
npiv enable 7-110
npv auto-load-balance disruptive 7-111
npv enable 7-112
port-security 7-113
port-security abort 7-115
port-security commit 7-116
port-security database 7-117
port-security distribute 7-119
port-security enable 7-120
port-track enable 7-121
port-track force-shut 7-122
port-track interface 7-123
purge fcdomain fcid 7-124
rlir preferred-cond fcid 7-125
rscn 7-127
rscn abort 7-128
rscn commit 7-129
rscn distribute 7-130
rscn event-tov 7-131
san-port-channel persistent 7-132
scsi-target 7-133
switchport 7-135
switchport ignore bit-errors 7-138
system default switchport 7-140
system default zone default-zone permit 7-142

Send comments to nx5000-docfeedback@cisco.com

system default zone distribute full 7-143
trunk protocol enable 7-144
vsan database 7-145
wwn secondary-mac 7-148
wwn vsan 7-149
zone clone 7-150
zone commit 7-151
zone compact 7-152
zone copy 7-153
zone default-zone 7-155
zone merge-control restrict vsan 7-156
zone mode enhanced 7-157
zone name (configuration mode) 7-158
zone name (zone set configuration submode) 7-160
zone rename 7-161
zoneset (configuration mode) 7-162
zoneset (EXEC mode) 7-164

CHAPTER 8 Cisco Nexus 5000 Series Fibre Channel Show Commands 8-1

show cfs 8-2
show debug npv 8-4
show device-alias 8-5
show fabric-binding 8-7
show fc2 8-9
show fcalias 8-11
show fcdomain 8-12
show fcdroplatency 8-14
show fcflow stats 8-15
show fcid-allocation 8-16
show fcns database 8-17
show fcns statistics 8-19
show fcoe 8-20
show fcroute 8-21
show fcs 8-23
show fcsp 8-25
show fctimer 8-27

Send comments to nx5000-docfeedback@cisco.com

show fdmi 8-29
show flogi 8-30
show fspf 8-32
show in-order-guarantee 8-33
show interface 8-34
show loadbalancing 8-36
show lldp 8-37
show npv flogi-table 8-40
show npv status 8-41
show port index-allocation 8-42
show port-security 8-43
show rlir 8-45
show rscn 8-46
show san-port-channel 8-47
show scsi-target 8-49
show topology 8-51
show trunk protocol 8-52
show vig 8-53
show vsan 8-54
show wwn 8-56
show zone 8-57
show zone analysis 8-59
show zoneset 8-62

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 Command Reference, Release 4.0*. It also provides information on how to obtain related documentation.

This chapter includes the following sections:

- Audience, page xvii
- Organization, page xvii
- Document Conventions, page xviii
- Related Documentation, page xviii
- Obtaining Documentation and Submitting a Service Request, page xix

Audience

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

Organization

This reference is organized as follows:

Chapter	Title	Description
Chapter 1	Cisco Nexus 5000 Series Basic System Commands	Describes the basic Cisco NX-OS system commands. These commands allow you to navigate and control the switch.
Chapter 2	Cisco Nexus 5000 Series Ethernet Commands	Describes the Cisco NX-OS Ethernet and Virtual Ethernet commands.
Chapter 4	Cisco Nexus 5000 Series Quality of Service Commands	Describes the Cisco NX-OS quality of service commands.
Chapter 5	Cisco Nexus 5000 Series Security Commands	Describes the Cisco NX-OS security commands.
Chapter 6	Cisco Nexus 5000 Series System Management Commands	Describes the Cisco NX-OS system management commands.

Send comments to nx5000-docfeedback@cisco.com

Chapter	Title	Description
Chapter 7	Cisco Nexus 5000 Series Fibre Channel Commands	Describes the Cisco NX-OS Fibre Channel and virtual Fibre Channel commands.
Chapter 8	Cisco Nexus 5000 Series Fibre Channel Show Commands	Describes the Cisco NX-OS Fibre Channel show 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]	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.

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:

Send comments to nx5000-docfeedback@cisco.com

Cisco Nexus 5000 Series CLI Software Configuration Guide, Cisco NX-OS Release 4.0

Cisco Nexus 5000 Series NX-OS Command Reference, Cisco NX-OS Release 4.0

Cisco Nexus 5000 Series Hardware Installation Guide

Cisco Nexus 5000 Series System Messages Reference

Cisco Nexus 5000 Series Release Notes

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide, Cisco NX-OS Release 4.1

Cisco Nexus 2000 Series Fabric Extender Hardware Installation Guide

Cisco Nexus 5000 Series Fabric Manager Software Configuration Guide, Cisco NX-OS Release 4.0

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

Cisco Nexus 5000 Series 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	The delimiter character 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) 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

Interface 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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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.

Usage Guidelines None.

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.

Usage Guidelines None.

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.

Usage Guidelines

None.

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
```

Send comments to nx5000-docfeedback@cisco.com

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

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

Related Commands

Command	Description
show clock	Displays 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 the 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 terminal

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

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.
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.

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.

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*

Send comments to nx5000-docfeedback@cisco.com

Table 1-2 URL Prefix Keywords for Remote File Systems (continued)

Keyword	Source or Destination
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.

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.

Send comments to nx5000-docfeedback@cisco.com

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 host name.

This section contains usage guidelines for the following topics:

- Copying Files from a Server to Bootflash Memory, page -21
- Copying a Configuration File from a Server to the Running Configuration, page -21
- Copying a Configuration File from a Server to the Startup Configuration, page -21
- Copying the Running or Startup Configuration on a Server, page -21

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 having 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:
```

Send comments to nx5000-docfeedback@cisco.com

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:

```
switch# copy scp://10.10.1.1/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. Once this command is entered, the running and the startup copies of the configuration are identical.

copy running-config startup-config

Syntax Description

This command has no additional 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.

Examples

The following example shows saving 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

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.

Usage Guidelines

None.

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
```

Related Commands

Command	Description
dir	Displays the contents of a directory.

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 in configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

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

In the following example, the **end** command is used to exit from interface configuration mode and return to EXEC mode. A **show** command is used in EXEC mode 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

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 in EXEC mode.

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.

Usage Guidelines

None.

Examples

In the following example, 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

The following 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 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 feature 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.

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 that LLDP 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:	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.

Usage Guidelines

None.

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

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**.

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*

Send comments to nx5000-docfeedback@cisco.com

Table 1-5 URL Prefix Keywords for Remote File Systems

Keyword	Source or Destination
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*

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

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.

You can use **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.

This command only installs Cisco NX-OS software on devices with dual supervisor modules. To install new software on a switch with a single supervisor, you must use the **reload** command.

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@10.10.1.1/nx-os_kick.bin system
bootflash:scp://adminuser@10.10.1.1/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.

Usage Guidelines

None.

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

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

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

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 init-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

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** {**management** | *vrf_name*}]

Syntax Description

dest-address	IPv4 address of destination device. 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.
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 {**management** | *vrf_name*}	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive. The default is the default 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.

Usage Guidelines

None.

Examples

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

```
switch# ping 172.28.231.246
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
traceroute	Displays the routes that packets take when traveling to an IP address.

Send comments to nx5000-docfeedback@cisco.com

reload

To reload the entire Cisco Nexus 5000 Series switch, use the **reload** command.

reload

Syntax Description

This command has no arguments or keywords,

Command Default

Reloads the entire device.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

The **reload** command disrupts traffic on the device.

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
```

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.

Usage Guidelines

None.

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

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

Command History

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

Usage Guidelines

None.

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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) Displays the 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.

Usage Guidelines

None.

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 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.

Usage Guidelines

None.

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.

Usage Guidelines None.

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 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.

Usage Guidelines

None.

Examples

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

```
switch# show copyright
```

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.

Usage Guidelines

None.

Examples

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

```
switch# show environment
```

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

```
switch# show environment power
```

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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
```

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.

Usage Guidelines

None.

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 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.

Usage Guidelines

None.

Examples

This example shows how to display the installation failure reason:

```
switch# show install all failure-reason
```

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
```

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

Syntax Description

This command has no arguments or keywords.

Command Default

Displays all hardware inventory information.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None.

Examples

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

```
switch# show inventory
```

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.

Usage Guidelines

None.

Examples

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

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

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

```
switch# show license brief
```

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

```
switch# show license
```

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 (:).

Examples

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

```
switch# show license host-id
```

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) Displays a 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.

Usage Guidelines

None.

Examples

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

```
switch# show license usage
```

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

```
switch# show license usage FC_FEATURES_PKG
```

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**]

Syntax Description

console	(Optional) Displays only information about the console port configuration.

Command Default

Displays information about the the terminal port configuration.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None.

Examples

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

```
switch# show line
```

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

```
switch# show line console
```

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*]

Syntax Description

module_number	(Optional) Number of the module. The valid range is from 1 to 3.

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.

Usage Guidelines

None.

Examples

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

```
switch# show module
```

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

```
switch# show module 2
```

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.

Usage Guidelines

None.

Examples

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

```
switch# show processes
```

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.

Usage Guidelines

None.

Examples

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

```
switch# show processes cpu
```

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.

Usage Guidelines

None.

Examples

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

```
switch# show processes log
```

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

```
switch# show processes log details
```

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

```
switch# show processes log pid 3632
```

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.

Usage Guidelines

None.

Examples

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

```
switch# show processes memory
```

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

```
switch# show processes memory shared
```

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.

Usage Guidelines

None.

Examples

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

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

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 1-6 describes the notations used in the command output.

Table 1-6 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 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
```

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 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** | **module** *module_number* | **powersupply** *powersupply_number* | **sup**}

Syntax Description

all	Displays the SPROM contents for all components on the physical device.
backplane	Displays the SPROM contents for the backplane.
module *module_number*	Displays the SPROM contents for a I/O module. The module number range is from 1 to 3.
powersupply *powersupply_number*	Displays the SPROM contents for a power supply. The power supply number range 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.

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
```

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

```
switch# show sprom backplane
```

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.

Usage Guidelines

None.

Examples

This example shows how to display the startup configuration:

```
switch# show startup-config
```

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
```

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

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

None.

Examples

This example shows how to display the reset-reason history for the switch:

```
switch# show system reset-reason
```

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.

Usage Guidelines

None.

Examples

This example shows how to display the amount of time since the last system restart:

```
switch# show system uptime
```

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.

Examples

This example shows how to display technical support information:

```
switch# show tech-support
```

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
```

This example shows how to display the technical support information for a specific feature:

```
switch# show tech-support aaa
```

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.

Usage Guidelines

None.

Examples

This example shows how to display information about the terminal configuration for a session:

```
switch# show terminal
```

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 [**image** *filename*]

Syntax Description

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.

Usage Guidelines

None.

Examples

This example shows how to display the version information for the kickstart and system image running on the device:

```
switch# show version
```

This example shows how to display the version information for an image file:

```
switch# show version image bootflash:old_image
```

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

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

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

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	The URL for the destination file system and file. Use the following format: [//*server*[:*port*]][/*path*/]*filename*
vrf management	(Optional) Specifies to use the default 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.

Usage Guidelines

None.

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

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

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.

Usage Guidelines

None.

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.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
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 type xterm
```

This example shows how to revert to the default terminal type:

```
switch# terminal no 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** {**management** | *vrf_name*}] [**source** *src_addr*]

Syntax Description

dest_ddr	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 {**management** | *vrf_name*}	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive.
source *src_addr*	(Optional) Specifies a source IP address. The format is *A.B.C.D*.

Command Default

None.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to discover a route to a network device:

```
switch# traceroute 172.28.255.18 vrf management
```

Related Commands

Command	Description
ping	Displays the network connectivity to another network device.

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.

Usage Guidelines

None.

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

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 2

Cisco Nexus 5000 Series Ethernet Commands

This chapter describes the Cisco NX-OS Ethernet and virtual Ethernet commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

channel-group (Ethernet configuration)

To assign and configure a physical interface to a port channel group, 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 port channel associated with this channel group if the port channel does not already exist.
mode	(Optional) Specifies the port channel mode of the interface.
active	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. Interface is in active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
on	This is the default channel mode. All port channels 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**. A port channel in the **on** channel mode is a pure port channel and can aggregate a maximum of eight ports. The port channel does not run LACP.

You cannot change the mode for an existing port channel or any of its interfaces if that port channel 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 port channel. When you delete the last physical interface from a port channel, the port channel remains. To delete the port channel 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 port channels, that is, without a configured aggregation protocol. You can only add interfaces configured with the channel mode as **active** or **passive** to port channels 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 port channel.

When the interface joins a port channel, some of its individual parameters are overridden with the values on the port channel, 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 port channel:

- Description
- Cisco Discovery Protocol (CDP)
- LACP port priority
- Debounce

Send comments to nx5000-docfeedback@cisco.com

- Rate mode
- Shutdown
- SNMP trap

If interfaces are configured for the port channel interface and a member port is removed from the port channel, the configuration of the port channel interface is not propagated to the member ports.

Any configuration changes that you make in any of the compatibility parameters to the port channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel 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 port-channel interface.
show lacp	Displays LACP information.
show port-channel summary	Displays information on the port channels.

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 a specific counter to clear.

Command Default None.

Command Modes Any command mode

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

Usage Guidelines None.

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 dynamic

To clear dynamic entries from the forwarding table, use the **clear mac dynamic** command.

clear mac 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 vethernet. Specify the appropriate slot or virtual interface group number and port number.
port-channel *number*	(Optional) Specifies the port channel for which MAC addresses should be removed from the table. Use the port channel number.
vlan *vlan_id*	(Optional) Specifies the VLAN from which MAC addresses should be removed from the table. The range of valid values is from 1 to 4094.

Command Default

None.

Command Modes

Any command mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to clear all the dynamic entries from the MAC address table:

```
switch# clear mac dynamic
```

This example shows how to clear a dynamic entry for VLAN 2 from the MAC address table:

```
switch# clear mac dynamic address 001b.2106.58bc vlan 2
```

This example shows how to clear all dynamic entries for a virtual Ethernet from the MAC address table:

```
switch# clear mac dynamic interface vethernet 1/1
```

This example shows how to clear all dynamic entries for VLAN 2 from the MAC address table:

```
switch# clear mac dynamic vlan 2
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show mac dynamic	Displays the dynamic addresses in 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 vethernet. Specify the appropriate slot or virtual interface group number and port number.
port-channel *number*	(Optional) Specifies the port channel for which MAC addresses should be removed from the table. Use the port channel number.
vlan *vlan_id*	(Optional) Specifies the VLAN from which MAC addresses should be removed from the table. The range of valid values is from 1 to 4094.

Command Default

None.

Command Modes

Any command mode

Command History

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

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 in configuration mode.

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
```

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
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show mac-address-table	Displays the information about the MAC address table.

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 other arguments or keywords.

Command Default

None.

Command Modes

Any command mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to discard the NTP 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

Any command mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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

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-num* | **port-channel** *channel-num* | **vethernet** *interface-num*}] [**vlan** *vlan-id*]

Syntax Description

interface	(Optional) Specifies the interface type.
ethernet *interface-num*	Slot and port number.
port-channel *channel-num*	Port-channel number.
vethernet *interface-num*	Slot and port number.
vlan *vlan-id*	(Optional) Specifies the VLAN. The range is from 1 to 4094.

Command Default

None.

Command Modes

Any command 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* | **vethernet** *interface*}]

Syntax Description

interface	(Optional) Specifies the interface type.
ethernet *interface*	Slot and port number.
port-channel *channel*	Port-channel number.
vethernet *interface*	Slot and port number.

Command Default

None.

Command Modes

Any command 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

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

Configuration mode

Command History

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

Usage Guidelines

You must use the **feature interface-vlan** or the **svi enable** 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.

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

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 port channels on the switch before you can disable LACP.

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

Examples

This example shows how to enable LACP port channeling on the switch:

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

Related Commands

Command	Description
show lacp	Displays information on LACP.

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

None.

Command Default

Private VLANs are disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

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 PVLAN 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.

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 of valid values is from 0 to 4094.
vlan *vlan-id*	Number of the VLANs that you are mapping to the specified MSTI; the range of valid values 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 a 10-Gigabit Ethernet IEEE 802.3 interface, use the **interface ethernet** command.

interface ethernet *slot/port*

Syntax Description

slot	Specifies a slot from 1 to 3. The following list defines the slots available: • Slot 1 includes all the fixed ports. • 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	Specifies the port number within a particular slot.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enter configuration modefor Ethernet interface 1/4:

```
switch(config)# interface ethernet 1/4
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
show interface ethernet	Displays various parameters of a 10-Gigabit Ethernet IEEE 802.3 interface.

Send comments to nx5000-docfeedback@cisco.com

interface port-channel

To create a port-channel interface and enter interface configuration mode, use the **interface port-channel** command. To remove a logical port-channel interface or subinterface, 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 port-channel logical interface. The range of valid values is from 1 to 4096.

Command Default

None.

Command Modes

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 port-channel interface.
- If you do not assign a static MAC address on the port-channel 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 port channel 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 a port-channel group interface with channel-group number 50:

```
switch(config)# interface port-channel 50
switch(config-if)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show interface port-channel	Displays information on traffic on the specified port-channel interface.
show lacp	Displays LACP information.
show port-channel summary	Displays information on the port channels.

Send comments to nx5000-docfeedback@cisco.com

interface vethernet

To enter interface configuration mode for a virtual Ethernet interface, use the **interface vethernet** command.

interface vethernet *vig-num*/*port*

Syntax Description

vig-num	Specifies the virtual interface group (VIG) number. You must have previously created the VIG.
port	The only valid number for the port is 1.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enter configuration mode for virtual Ethernet interface 16/1:

```
switch(config)# interface vethernet 16/1
switch(config-if)#
```

Related Commands

Command	Description
interface ethernet	Configures a 10-Gigabit Ethernet IEEE 802.3 interface.
show interface vethernet	Displays various parameters of a virtual Ethernet interface.

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 other 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.

Usage Guidelines

None.

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

The valid values for *parameter* are as follows:

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 port channel.
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

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, port channel, or virtual Ethernet.

Examples

This example shows how to shows 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 172.20.52.106
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 230.0.0.1 interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface vethernet 4/1
```

Related Commands

Command	Description
show ip igmp snooping	Displays 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 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

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 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

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	Specifies the 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

EXEC mode

Command History

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

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 aging time has been changed.

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 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

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to configure 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 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** {*type slot/port* | **port-channel** *number*} [**auto-learn**]

no mac-address-table static *mac_address* {**vlan** *vlan_id*}

Syntax Description

mac_address	Specifies the MAC address to add to the table. Use the format EEEE.EEEE.EEEE.
vlan *vlan_id*	Specifies the VLAN to apply static MAC address; valid values are from 1 to 4094.
drop	Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
interface *type slot/port*	Specifies the interface. The type can be either ethernet or vethernet. Specify the appropriate slot or virtual interface group number and port number.
port-channel *number*	Specifies the interface. Use the port channel number.
auto-learn	(Optional) Allows moving of this MAC address.

Command Default

None.

Command Modes

Configuration mode

Command History

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

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.

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
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show mac-address-table	Displays information about MAC address table.

Send comments to nx5000-docfeedback@cisco.com

monitor session

Create a new SPAN session configuration or add to an existing session configuration with the **monitor session** command. To clear SPAN sessions, use the **no** form of this command.

monitor session {*number* | **all**} [**suspend**]

no monitor session {*number* | **all**} [**suspend**]

Syntax Description

number	Specifies the SPAN session to create or configure. Select session 1 to 18.
all	Specifies to apply configuration information to all SPAN sessions.
suspend	(Optional) Specifies to suspend the referenced SPAN session.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

This example shows how to create a SPAN session:

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

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

ntp

To configure the NTP peers and servers for the switch, use the **ntp** command. Use the **no** form of this command to remove configured peers and servers.

ntp {**peer** *hostname* | **server** *hostname*}

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

Syntax Description

peer *hostname*	The hostname or IP address of an NTP peer.
server *hostname*	The hostname or IP address of the NTP server.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

This example forms a server association with a server:

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

You can specify multiple associations. This example forms a peer association with a peer:

```
switch(config)# ntp peer 10.20.10.0
```

This example deletes an association with a peer:

```
switch(config)# no ntp peer 10.20.10.0
```

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 other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 the command.

ntp distribute

no ntp distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

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

The following 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 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.

Usage Guidelines

None.

Examples

The following 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

port-channel load-balance ethernet

To set 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

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 a port channel is going only to a single MAC address and you use the destination MAC address as the basis of port channel load balancing, the port channel always chooses the same link in that port channel; 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 port-channel 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.
4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

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.

Send comments to nx5000-docfeedback@cisco.com

A promiscuous port is defined as a private port that is assigned to a primary VLAN.

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 PVLAN 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 insolated 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 PVLAN 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 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 PVLAN 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 of valid values 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 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
```

This example shows how to explicitly enable BPDU Filtering on a virtual Ethernet interface:

```
switch (config)# interface vethernet 4/1
switch(config-if)# spanning-tree bpdufilter enable
```

Send comments to nx5000-docfeedback@cisco.com

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 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 **spanning-tree port type edge bpduguard default** 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 1 to 65536. • long—The range is 1 to 200,000,000.
auto	Sets the value of the port cost by the media speed of the interface (see to Table 2-1 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 2-1). See the **spanning-tree pathcost method** command for information on setting the path cost calculation method for Rapid PVST+.

Table 2-1 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.

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.

Send comments to nx5000-docfeedback@cisco.com

The port channel bundle is considered 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 additional arguments or keywords.

Command Default

Disabled.

Command Modes

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 Loop Guard command, **spanning-tree guard loop**, 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

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 CIST instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

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 of valid values is from 0 to 4094.
cost	Port cost for an instance; the range of valid values 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 port-channel bundle is considered 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 of valid values is from 4 to 30 seconds.

Command Default

15 seconds.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

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 of valid values is from 1 to 10 seconds.

Command Default

2 seconds.

Command Modes

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 of valid values is from 6 to 40 seconds.

Command Default

20 seconds.

Command Modes

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.

This command does not require a license.

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 of valid values is from 1 to 255 hops.

Command Default

20 hops.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

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; valid values are from 0 to 4094.
priority	Port priority for an instance; the range of valid values 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 port priority for 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 of valid values 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

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 of valid values 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, should the primary root fail.
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

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 (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 **spanning-tree mst simulate pvst global** 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) 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 (Rapid PVST+), use the **no spanning-tree mst simulate pvst global** command. To return to the default settings, which is seamless operation between MST and Rapid PVST+ on the switch, use the **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

Configuration mode

Interface 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

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 PVST+ spanning tree mode, which is the default mode. When you are using 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 **spanning-tree port type normal** command or the **no spanning-tree port type** command.

spanning-tree port type edge [**trunk**]

spanning-tree port type normal

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 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
```

Send comments to nx5000-docfeedback@cisco.com

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.
```

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 **spanning-tree port type normal** 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 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 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

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 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

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 **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

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 **spanning-tree port type normal** command or use the **no** form of this command.

spanning-tree port type network

spanning-tree port type normal

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

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 **spanning-tree port type normal** 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

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 of valid values is from 0 to 4094.
value	Port priority; valid values are 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 PVST+ spanning tree mode, which is the default STP mode. To configure the port priority for 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 range of valid values is from 0 to 4094.
forward-time *value*	(Optional) Specifies the STP forward-delay time; the range of valid values 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 of valid values 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 of valid values 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

Configuration mode

Command History

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

Usage Guidelines

Send comments to nx5000-docfeedback@cisco.com

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

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

Configuration mode

Command History

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

Usage Guidelines

You must use the **feature interface-vlan** or the **svi enable** 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; valid values are 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** interface configuration 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

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 additional keywords or arguments.

Command Default

None.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

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, that port 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.

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.

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.
4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

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 PVLAN 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 PVLAN 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 associate 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 the all private VLAN association 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

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 of valid values 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

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

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.
management	Specifies a configurable VRF name.

Command Default

None.

Command Modes

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

CHAPTER 3

Cisco Nexus 5000 Series 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 mac-address

To display the information about the MAC address, use the **show interface mac-address** command.

show interface [*type slot*/*port*] **mac-address**

Syntax Description

type slot/*port*	(Optional) Specifies the interface for which MAC addresses should be displayed. The type can be either ethernet or vethernet. Specify the appropriate slot or virtual interface group number and port number.

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
```

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 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
```

Related Commands

Command	Description
interface port-channel	Configures an EtherChannel interface.

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 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.

Usage Guidelines

None.

Examples

This example shows how to display information for all Ethernet and virtual Ethernet interfaces:

```
switch# show interface switchport
```

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 vlan

To display brief descriptive information about specified VLANs, use the **show interface vlan** command.

show interface vlan *vlan_id* [**brief** | **description** | **private-vlan mapping**]

Syntax Description

vlan_id	Number of the VLAN; the range of valid values is from 1 to 4094.
brief	(Optional) Summary information for the specified VLAN.
description	(Optional) Description of the specified VLAN.
private-vlan mapping	(Optional) 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 5
```

This example shows how to display a brief description for the specified VLAN:

```
switch# show interface vlan 5 brief
```

This example shows how to display the description for a specified VLAN:

```
switch# show interface vlan 5 description
```

This example shows how to display the private VLAN mapping information, if any, for the VLAN:

```
switch# show interface vlan 5 private-vlan mapping
```

When you specify a primary VLAN, the switch displays all secondary VLANs mapped to that primary VLAN.

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the status of the VLAN:

```
switch# show interface vlan 5 status
```

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. Valid values are 1 to 4094.
groups	(Optional) Displays information for 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.

Usage Guidelines

None.

Examples

This example shows how to display the IGMP snooping configuration of the switch:

```
switch# show ip igmp snooping
```

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 interface.
neighbor [**interface port-channel** *number*]	Displays information about the LACP neighbor. Optionally provide a port channel number.
port-channel [**interface port-channel** *number*]	Displays information about a port channel. Optionally provide a port channel number.
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
```

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 range of valid values 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

None.

Examples

This example shows how to display MAC address aging times:

```
switch# show mac-address-table aging-time
```

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** {*type 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 *type slot/port* | **port-channel** *number*	(Optional) Specifies the interface. Use either the type of interface (ethernet or vethernet), the slot number, and the port number, or the port-channel number.
vlan *vlan_id*	(Optional) Displays information for a specific VLAN; the range of valid values 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

None.

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
```

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	Shows notification messages about MAC addresses that were moved.
threshold	Shows 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.

Usage Guidelines

None.

Examples

This example shows how to display MAC address move notifications:

```
switch# show mac-address-table notification mac-move
```

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** {*type 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 *type slot*/*port* | **port-channel** *number*	(Optional) Specifies the interface. Use either the type of interface (ethernet or vethernet), the slot number, and the port number, or the port-channel number.
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 range of valid values 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

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 the information about the entries for the MAC address table:

```
switch# show mac address-table
```

This example shows how to display the 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 the information about the dynamic entries for the MAC address table:

```
switch# show mac address-table dynamic
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the 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 the static entries in the MAC address table:

```
switch# show mac address-table static
```

This example shows how to display the entries in the MAC address table for a specific VLAN:

```
switch# show mac address-table vlan 5
```

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 about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

show monitor session

To display information about the 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; valid values are 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; valid values are 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.

Usage Guidelines

None.

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
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for 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
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for 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
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for 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* [**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*.
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

Command History

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

Send comments to nx5000-docfeedback@cisco.com

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:

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.

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for EtherChannels.

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
```

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
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for 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
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures the load-balancing algorithm for 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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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 PVST+ or 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 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 PVST+ (configurable, default is short) and 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.

Examples

This example shows how to display spanning tree information:

```
switch# show spanning-tree
```

This example shows how to display the blocked ports in spanning tree:

```
switch(config)# show spanning-tree blockedports
```

This example shows how to determine if any ports are in any STP--inconsistent state:

```
switch# show spanning-tree inconsistentports
```

This example shows how to display the path cost method:

```
switch(config)# show spanning-tree pathcost method
```

Send comments to nx5000-docfeedback@cisco.com

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)
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 PVST+ or MST.

Related Commands

Command	Description
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays brief summary information about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays 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 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.

Usage Guidelines

None.

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 STP.
show spanning-tree bridge	Displays bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays brief summary information about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays status and configuration of the root bridge for the STP instance to which this switch belongs.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
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 status and configuration of the local 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 PVST+ or MST protocol is active.

Command Default

None.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None.

Examples

This example shows display STP information for the bridge:

```
switch# show spanning-tree bridge
```

Related Commands

Command	Description
show spanning-tree	Displays information 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 brief summary information about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays 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 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.

Usage Guidelines

None.

Examples

This example shows how to display a brief summary of STP information:

```
switch(config)# show spanning-tree brief
```

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays 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 STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays status and configuration of the root bridge for the STP instance to which this switch belongs.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
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 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.

Usage Guidelines

None.

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 STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays brief summary information about STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays status and configuration of the root bridge for the STP instance to which this switch belongs.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
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 STP interface status and configuration of specified interfaces, use the **show spanning-tree interface** command.

show spanning-tree interface {*interface slot/port* | **port-channel** *number*} [**active** [**brief** | **detail**] | **brief** [**active**] | **cost** | **detail** [**active**] | **edge** | **inconsistency** | **priority** | **rootcost** | **state**]

Syntax Description

interface *type slot/port* | **port-channel** *number*	Specifies the interface. Use either the type of interface (ethernet or vethernet) and its slot and port number, or the port-channel number.
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	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 MST, this command displays the PVST simulation setting.

Note If you are running MST, use the **show spanning-tree mst** command to show more detail on the specified interfaces.

Send comments to nx5000-docfeedback@cisco.com

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 bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays brief summary information about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays 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 MST status and configuration, use the **show spanning-tree mst** command.

show spanning-tree mst [*instance_id* [**detail** | **interface** {*interface slot*/*port* | **port-channel** *number*} [**detail**]]

show spanning-tree mst [**configuration** [**digest**]]

show spanning-tree mst [**detail** | **interface** {*interface slot*/*port* | **port-channel** *number*}} [**detail**]]

Syntax Description

instance_id	(Optional) The MST instance range that you want to display. For example, 0 to 3, 5, 7 to 9.
detail	(Optional) Displays detailed MST information.
interface slot/*port* | **port-channel** *number*	(Optional) Specifies the interface. Use either the type of interface (ethernet or vethernet) and its slot and port number, or the port-channel number.
configuration	(Optional) Displays current 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 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 MST instance information for the VLAN ports that are currently active:

```
switch# show spanning-tree mst
```

This example shows how to display STP information about a specific MST instance:

```
switch)# show spanning-tree mst 0
```

This example shows how to display detailed STP information about the MST protocol:

```
switch)# show spanning-tree mst detail
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display STP information about specified MST interfaces:

```
switch)# show spanning-tree mst interface ethernet 8/2
```

This example shows how to display information about the MST configuration:

```
switch)# show spanning-tree mst configuration
```

This example shows how to display the MD5 digest included in the current MST configuration:

```
switch)# show spanning-tree mst configuration digest
```

See Table 3-2 on page 3-28 for descriptions of the fields that are displayed in the output of **show spanning-tree** commands.

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays brief summary information about STP.
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.
show spanning-tree root	Displays 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 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 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.

Usage Guidelines

None.

Examples

This example shows how to display information for the root bridge:

```
switch(config)# show spanning-tree root
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays 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 STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about 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 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 PVST+ or 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 STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays 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 STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays 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

Send comments to nx5000-docfeedback@cisco.com

show spanning-tree vlan

To display 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** {*interface 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	Specifies the VLAN or range of VLANs that you want to display.
active	(Optional) Displays information about STP VLANs and active ports.
brief	(Optional) Displays 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 slot/port | **port-channel** *number*	(Optional) Specifies the interface. Use either the type of interface (ethernet or vethernet) and its slot and port number, or the port-channel number.
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	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.

Usage Guidelines

None.

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 STP.
show spanning-tree active	Displays information about STP active interfaces only.
show spanning-tree bridge	Displays bridge ID, timers, and protocol for the local bridge on the switch.
show spanning-tree brief	Displays brief summary information about STP.

Send comments to nx5000-docfeedback@cisco.com

Command	Description
show spanning-tree detail	Displays detailed information about STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.
show spanning-tree mst	Displays information about MST STP.
show spanning-tree root	Displays 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 other 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

None.

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 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 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 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	Specifies the 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.

Usage Guidelines

None.

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

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 4

Cisco Nexus 5000 Series Quality of Service Commands

This chapter describes the Cisco NX-OS quality of service commands available on Cisco Nexus 5000 Series switches.

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 *class-map-name*

no class-map *class-map-name*

Syntax Description

class-map-name	Name assigned to the class map. The name class default is reserved.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

You can define a class map for each class of traffic to be used in QoS policies.

No license required for this command.

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
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

match cos

To define a traffic class based on the Class of Service (CoS) value in the 802.1Q, use the **match cos** command. To remove the **match cos** configuration, use the no form of this command.

match cos *multi-range-cos-values*

no match cos *multi-range-cos-values*

Syntax Description

multi-range-cos-values	Specifies a list of multiple ranges of Class of Service (CoS) values. Values can range from 1 to 7.

Command Default

None.

Command Modes

Class-map configuration.

Command History

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

Usage Guidelines

You can create a traffic class based on CoS values in the 802.1Q or ISL header.

No license required for this command.

Examples

This example shows how to create a match on CoS:

```
switch(config)# class-map class_cos
switch(config-cmap)# match cos 2, 5-6
```

This example shows how to remove the match on CoS:

```
switch(config)# class-map class_cos
switch(config-cmap)# no match cos 2, 5-6
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.
show class-map	Displays class maps.

Send comments to nx5000-docfeedback@cisco.com

policy-map

To create or modify a policy map and enter the policy-map configuration mode, use the **policy-map** command. To remove a policy map, use the **no** form of this command.

policy-map *name*

no policy-map *name*

Syntax Description

name	Name assigned to the policy map.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

You can create a policy map based on class maps to define QoS actions to perform on packets.

You can configure the class in a policy-map and apply parameters. This example shows the parameters you can apply:

```
switch(config)# policy-map my_policy1
switch(config-pmap)# ?
class  Policy Criteria
switch(config-pmap)# class class1
switch(config-pmap-c)# ?
bandwidth  Specify bandwidth for the class
mtu        Configure the system class MTU
pause      Configure pause behavior
priority   Configure traffic class priority
```

Use the **service-policy** command to assign policy maps to interfaces or a system.

No license required for this command.

Examples

This example shows how to create or modify a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap)# class class1
switch(config-pmap-c)# mtu 9216
```

This example shows how to remove a policy map:

```
switch(config)# no policy-map my_policy1
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
class-map	Creates or modifies a table map.
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

service-policy

To associate the system class policy-map to the service policy for the system, use the **service-policy** command.

service-policy *[policy-map-name]*

no service-policy

To associate the system class policy-map to the interface, use the **service-policy** command.

service-policy output *[policy-map-name]*

no service-policy output

Syntax Description

policy-map-name	Name of the policy map to attach to this interface or system policy. Only one policy map can be attached to the input and one to the output of a given interface.

Command Default

No QoS policies are active on an interface until the **service-policy** command is entered.

Command Modes

Interface configuration

System qos

Command History

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

Usage Guidelines

No license required for the command.

Examples

This example shows how to attach policy maps to to use as the service policy for the system.:

```
switch# configure terminal
switch(config)# mtu 9216
switch(config)# system qos
switch(config-sys-qos)# service-policy policy-map1
```

The following example shows how to attach a policy map to an interface:

```
switch(config)# class-map best-effort-drop-class
switch(config-cmap)# match cos 5
switch(config)# policy-map policy_map1
switch(config-pmap)# class best-effort-drop-class
switch(config-pmap-c)# mtu 9216
switch(config)# interface eth1/1
switch(config-if)# service-policy output policy_map1
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
class-map	Creates or modifies a class map.
policy-map	Creates or modifies a policy map.
show policy-map	Displays policy maps.

Send comments to nx5000-docfeedback@cisco.com

system jumbomtu

To define the upper bound of any MTU in the system, use the **system jumbomtu** command.

system jumbomtu [value]

Syntax Description

value	The jumbomtu value. The range is 2240-9216.

Command Default

9216 bytes

Command Modes

Global configuration

Command History

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

Usage Guidelines

No license required for this command.

Examples

This example shows how to define the upper bound of any MTU in the system:

```
switch(config)# system jumbomtu 9216
```

Send comments to nx5000-docfeedback@cisco.com

system qos

To configure system policy or set multicast-cos option, use the **system qos** command.

system qos

Syntax Description

None.

Command Default

None.

Command Modes

Global configuration

Command History

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

Usage Guidelines

No license required for the command.

Examples

This example shows how to configure a system qos:

```
switch# configure terminal
switch(config)# system qos
switch(config-sys-qos)# service-policy policy-map1
```

Related Commands

Command	Description
service- policy	Associates the system class policy-map to the service policy for the system
set multicast-cos	Sets the Class of Service (CoS) value associated with the multicast system class.

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**}

Syntax Description

auto	Negotiates PFC capability.
on	Force-enables PFC.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

No license required for the command.

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
```

Send comments to nx5000-docfeedback@cisco.com

show class-map

To display class maps, use the **show class-map** command.

show class-map [*name*]

Syntax Description

name	(Optional) Specifies the class map to display.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

You can display all class maps if a name is not specified. Otherwise, the class map specified is displayed. No license required for the command.

Examples

This example shows how to display a class map:

```
switch# show class-map my_class_map
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.

Send comments to nx5000-docfeedback@cisco.com

show policy-map

To display policy maps, use the **show policy-map** command.

show policy-map [*name*]

Syntax Description		
	name	(Optional) Specifies the policy-map name to display.

Command Default None.

Command Modes Global configuration.

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

Usage Guidelines You can display all policy maps if a name is not specified. Otherwise, the policy map specified is displayed.

No license required for this command.

Examples This example shows how to display a policy map:

```
switch# show policy-map my_policy_map
```

Related Commands	Command	Description
	class-map	Creates or modifies a class map.
	policy-map	Creates or modifies a policy map.

Send comments to nx5000-docfeedback@cisco.com

show system qos

To display system QoS information, use the **show system qos** command.

show system qos

Syntax Description

None.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

No license required for the command.

Examples

This example shows how to display system QoS information:

```
switch(config)# show system qos
```

Related Commands

Command	Description
system qos	Configures the system class QoS.

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 [*name*] **priority-flow-control**

Syntax Description

name	(Optional) Name of the interface.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

No license required for the command.

Examples

This example shows how to display the priority flow control details for a specified interface:

```
switch(config)# show interface ethernet 1/1 priority-flow-control
---------------------------------------
Port       Mode Oper RxPPP      TxPPP
---------------------------------------
Eth1/1     auto off  0          0
```

The interface specified is Eth1/1, the PFC mode is set to negotiate PFC capability, the operation is off and packets transmitted is zero.

Related Commands

Command	Description
priority-flow-control	Sets the PFC mode for the selected interface.

Send comments to nx5000-docfeedback@cisco.com

show policy-map interface

To display the system policy configured on the system and per class statistics, use the **show policy-map interface** command.

show policy-map interface [*name*]

Syntax Description

name	(Optional) Name of the interface.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

This command provides per class statistics.

No license required for the command.

Examples

This example shows the per class pause statistics displayed for a default system class:

```
switch(config)# show policy-map interface ethernet 3/1
```

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

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 5

Cisco Nexus 5000 Series 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

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, of **local** method or both and they fail, then the accounting authentication fails.

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 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	Specifies a 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

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 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 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	Specifies a 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

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)# 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 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

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 (MSCHAP) 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

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enable MSCHAP authentication:

```
switch(config)# aaa authentication login mschap enable
```

This example shows how to disable MSCHAP authentication:

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the status of MSCHAP authentication.

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

Configuration mode

Command History

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

Usage Guidelines

None.

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

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 creates a VLAN access map named vlan-map-01, assigns an IPv4 ACL named ip-acl-01 to the map, specifies that the switch forwards packets matching the ACL, and enables 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.

Command Default

None.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None.

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.

Usage Guidelines

None.

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

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 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 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 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 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 matches only packets that have a 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:

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows:

  addrgroup *address-group-name*

  The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

  ```
  switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
  ```

- 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

  The following 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

  The following 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.

Send comments to nx5000-docfeedback@cisco.com

The following 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.

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

Send comments to nx5000-docfeedback@cisco.com

- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **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)

Send comments to nx5000-docfeedback@cisco.com

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)

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)

Send comments to nx5000-docfeedback@cisco.com

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 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 (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

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

  The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  The following 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 characters.

Command Default

None.

Command Modes

User role configuration

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
```

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	The switch feature name as listed in the **show role feature** command output.

Command Default

None.

Command Modes

User role feature group configuration

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 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

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

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.

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

Command History

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

Usage Guidelines

None.

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. Can be up to 64 characters long. Names cannot contain a space or quotation mark.

Command Default

No IPv4 ACLs are defined by default.

Command Modes

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

in

Command Modes

Interface configuration

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 Ethernet port-channel interfaces

You can also use the **ip port access-group** command to apply an IPv4 ACL as a port ACL to the following interface types:

- Tunnels
- Loopback interfaces
- Management 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.

Send comments to nx5000-docfeedback@cisco.com

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
```

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

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 ACL.

Command Default

No MAC ACLs are defined by default.

Command Modes

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

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 Ethernet port-channel interfaces

You can also apply a MAC ACL as a VLAN ACL. For more information, see the match, page 40.

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
```

Send comments to nx5000-docfeedback@cisco.com

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
```

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	The specified ACL is an IPv4 ACL.
ipv6	Configures IPv6 features
mac	The specified ACL is a MAC ACL.
address *access-list-name*	Specifies the ACL.

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.

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 creates a VLAN access map named vlan-map-01, assigns an IPv4 ACL named ip-acl-01 to the map, specifies that the switch forwards packets matching the ACL, and enables 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 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 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 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 matches only packets that have a 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

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:

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows:

  addrgroup *address-group-name*

  The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

  ```
  switch(config-acl)# permit ip any addrgroup lab-gateway-svrs
  ```

- 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

  The following 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

  The following 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.

Send comments to nx5000-docfeedback@cisco.com

The following 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.

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

Send comments to nx5000-docfeedback@cisco.com

- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **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)

Send comments to nx5000-docfeedback@cisco.com

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)

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)

Send comments to nx5000-docfeedback@cisco.com

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 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 (MAC)

To create a MAC 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

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
```

The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

```
switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
```

The following 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
```

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

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

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

Command History

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

Usage Guidelines

None.

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

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

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

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 maximum length is 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	Configures a preshared key to authenticate communication between the RADIUS client and server. The maximum length is 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 maximum size is 32 characters.

Send comments to nx5000-docfeedback@cisco.com

username *name*	Specifies a username in the test packets. The maximum size is 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

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 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 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 maximum length is 63 characters.

Command Default

Clear text authentication.

Command Modes

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

Configuration mode

Command History

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

Usage Guidelines

None.

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

Configuration mode

Command History

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

Usage Guidelines

None.

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
MAC ACL configuration

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

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.

Send comments to nx5000-docfeedback@cisco.com

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

IP access list ip-acl-01
        7 permit tcp 128.0.0/16 any eq www
        10 permit udp 128.0.0/16 any
        13 permit icmp 128.0.0/16 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 128.0.0/16 any eq www
        110 permit udp 128.0.0/16 any
        120 permit icmp 128.0.0/16 any eq echo
        130 deny igmp any any
```

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

Configuration mode

Command History

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

Usage Guidelines

None.

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
```

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

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 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.

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 maximum length is 256 characters.

Command Default

None.

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 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 10.10.1.1
```

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 10.10.1.1
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to add a server to a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

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 10.10.2.2
```

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 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.

Usage Guidelines

None.

Examples

This example shows how to display the configuration of the accounting log:

```
switch# show aaa accounting
```

Send comments to nx5000-docfeedback@cisco.com

show aaa authentication

To display 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 MS-CHAP enable configuration.

Command Default

None.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None.

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 MSCHAP configuration:

```
switch# show aaa authentication login mschap
```

Send comments to nx5000-docfeedback@cisco.com

show aaa groups

To display 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.

Usage Guidelines

None.

Examples

This example shows how to display AAA group information:

```
switch# show aaa groups
```

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 to show.

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.

Usage Guidelines

None.

Examples

This example shows how to 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) The 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.

Usage Guidelines

None.

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
```

Send comments to nx5000-docfeedback@cisco.com

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 to show.

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
```

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 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 to show.

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.

Usage Guidelines

None.

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 maximum character size is 256.
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 10.10.1.1
```

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 10.10.1.1
```

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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, 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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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 accouting (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.

Usage Guidelines

None.

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.

Usage Guidelines

None.

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, 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.

Usage Guidelines

None.

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 10.10.2.2
```

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 10.10.2.2
```

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.

Usage Guidelines

None.

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) Displays 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.

Usage Guidelines None.

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.

Usage Guidelines

None.

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 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.

Usage Guidelines

None.

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 on a Cisco Nexus 5000 Series switch, use the **ssh** command.

ssh [*username*@]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Username for the SSH session.
ipv4-address	IPv4 address of the remote switch.
hostname	Hostname of the remote switch.
vrf *vrf-name*	(Optional) Specifies the VRF name to use for the SSH session.

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 10.10.1.1 vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
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

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
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to remove the DSA SSH server key:

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
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

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*	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

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	Specifies the time interval in minutes. The range is from 1 to 1440.

Command Default

0 minutes.

Command Modes

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 to send authentication requests to a specific TACACS+ server when logging in, use the **radius-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

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 in configuration mode. 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 maximum character size is 256.
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	Configures a preshared key to authenticate communication between the TACACS+ client and server. The maximum length is 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 maximum size is 32.
username *name*	(Optional) Specifies a user name in the test packets. The maximum size is 32.
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.

Test username: test.

Test password: test.

Send comments to nx5000-docfeedback@cisco.com

Command Modes

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 10.10.2.3 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 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 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 maximum length is 63 characters.

Command Default

None.

Command Modes

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

The following example shows how to 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

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*]

Syntax Description

ipv4-address	IPv4 address of the remote switch.
hostname	Hostname of the remote switch.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the VRF name to use for the Telnet session.

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

None.

Examples

This example shows how to start a Telnet session using IPv4:

```
switch# telnet 10.10.1.1 vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet server enable	Enables the Telnet server.

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

Configuration mode

Command History

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

Usage Guidelines

None.

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

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*

no use-vrf *vrf-name*

Syntax Description

vrf-name	Specifies VRF instance name.

Command Default

None.

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 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.
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.
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

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
- 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.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to create a user account with a password:

```
switch(config)# username user1 password Ci5co321
```

This example shows howto 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.

Command Default

None.

Command Modes

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

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

Command History

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

Usage Guidelines

None.

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 enter virtual forwarding and routing instance (VRF) policy configuration mode for a user role, use the **vrf policy deny** command. To revert to the default VRF policy 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.

Command History

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

Usage Guidelines

None.

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

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 6

Cisco Nexus 5000 Series System Management Commands

This chapter describes the system management commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

clear logging nvram

Use the **clear logging nvram** command to clear the NVRAM logs.

clear logging nvram

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to clear the NVRAM logs:

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

Related Commands

Command	Description
show logging nvram	Displays the NVRAM logs.

Send comments to nx5000-docfeedback@cisco.com

clear logging onboard

To clear the 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

Any.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to clear the OBFL environmental history entries:

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

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

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

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

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

The following example shows how to clear the OBFL stack trace entries:

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

Related Commands

Command	Description
show logging onboard	Displays onboard failure logs.

Send comments to nx5000-docfeedback@cisco.com

clear logging session

Use the **clear logging session** command to clear the current logging session.

clear logging session

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to clear the current logging session:

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

Related Commands

Command	Description
show logging session	Displays logging session status.

Send comments to nx5000-docfeedback@cisco.com

logging console

Use the **logging console** command to enable logging messages to the console session.

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) The 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.

Command History

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

Usage Guidelines

None.

Examples

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

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

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

Send comments to nx5000-docfeedback@cisco.com

logging level

Use the **logging level** command to enable logging messages from the defined facility that have the specified severity level or higher.

To disable logging messages from the defined facility, use the **no** form of this command.

logging level *facility severity-level*

no logging level *facility severity-level*

Syntax Description

facility	Defines the appropriate *facility*. The facilities are listed in the "System Message Logging Facilities" section on page 35. To apply the same severity level to all facilities, use the **all** facility.
severity-level	The 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.

Command History

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

Usage Guidelines

None.

Examples

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

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

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

Use the **logging logfile** command to configure the name of the log file used to store system messages and the minimum severity level to log.

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	Configure the name of the log file to be used to store system messages.
severity-level	The 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.

Command History

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

Usage Guidelines

None.

Examples

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

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

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show logging logfile	Displays the log file.

Send comments to nx5000-docfeedback@cisco.com

logging module

Use the **logging module** command to enable module log messages. Set a specified severity level or use the default.

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

logging module [*severity-level*]

no logging module

Syntax Description

severity-level	(Optional) The 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.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enable module log messages:

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

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show logging module	Displays the module logging status.

Send comments to nx5000-docfeedback@cisco.com

logging monitor

Use the **logging monitor** command to enable the device to log messages to the monitor (terminal line). This configuration applies to Telnet and SSH sessions.

To disable monitor log messages, use the **no** form of this command.

logging monitor [*severity-level*]

no logging monitor

Syntax Description

severity-level	(Optional) The 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.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enable monitor log messages:

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

Send comments to nx5000-docfeedback@cisco.com

Related Commands

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

Send comments to nx5000-docfeedback@cisco.com

logging server

Use the **logging server** command to configure a remote syslog server at the specified host name or IPv4/IPv6 address.

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**}]

no logging server *host*

Syntax Description

host	Configure the host name or IPv4/IPv6 address of the Remote Syslog Server.
severity-level	(Optional) The 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) Define the appropriate outgoing *facility*. The facilities are listed in the System Message Logging Facilities section. The default outgoing facility is **local7**.

Command Default

The default outgoing facility is **local7**.

Command Modes

Global configuration

Command History

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

Usage Guidelines

None.

Send comments to nx5000-docfeedback@cisco.com

Examples

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

```
switch# configure terminal
switch(config)# logging server 172.28.254.253
switch(config)#
```

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

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

Related Commands

Command	Description
show logging server	Displays the configured syslog servers.

Send comments to nx5000-docfeedback@cisco.com

logging timestamp

Use the **logging timestamp** command to set the logging timestamp units. By default, the units are seconds.

To reset the logging timestamp 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 | **milliseconds** | **seconds**	Selects the units to use for logging timestamps. The default units are **seconds**.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to set the logging timestamp units to microseconds:

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

Related Commands

Command	Description
show logging timestamp	Displays the logging timestamp configuration.

Send comments to nx5000-docfeedback@cisco.com

show logging console

Use the **show logging console** command to display the console logging configuration.

show logging console

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the console logging configuration:

```
switch# show logging console
switch#
```

Related Commands

Command	Description
logging console	Configures logging to the console.

Send comments to nx5000-docfeedback@cisco.com

show logging info

Use the **show logging info** command to display the logging configuration.

show logging info

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the logging configuration:

```
switch# show logging info
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show logging last

Use the **show logging last** command to display the last number of lines of the logfile.

show logging last *number*

Syntax Description		
	number	Enters the number of lines to display from 1 to 9999.

Command Default None.

Command Modes Any.

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

Usage Guidelines None.

Examples This example shows how to display the last 42 lines of the log file:

```
switch# show logging last 42
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show logging level

Use the **show logging level** command to display the facility logging severity level configuration.

show logging level [*facility*]

Syntax Description

facility	(Optional) Defines the appropriate logging *facility*. The facilities are listed in the System Message Logging Facilities section.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the port-channel logging severity level configuration:

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

Related Commands

Command	Description
logging level	Configures the facility logging level.

Send comments to nx5000-docfeedback@cisco.com

show logging logfile

Use the **show logging logfile** command to display the messages in the log file that were timestamped within the span entered. If you do not enter an end time, the current time is used.

show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]

Syntax Description

start-time	(Optional) Enter 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	(Optional) Enter 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

Any.

Command History

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

Usage Guidelines

None.

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
switch#
```

Related Commands

Command	Description
logging logfile	Configures logging to a log file.

Send comments to nx5000-docfeedback@cisco.com

show logging module

Use the **show logging module** command to display the module logging configuration.

show logging module

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the module logging configuration:

```
switch# show logging module
switch#
```

Related Commands

Command	Description
logging module	Configures module logging.

Send comments to nx5000-docfeedback@cisco.com

show logging monitor

Use the **show logging monitor** command to display the monitor logging configuration.

show logging monitor

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the monitor logging configuration:

```
switch# show logging monitor
switch#
```

Related Commands

Command	Description
logging monitor	Configures logging on the monitor.

Send comments to nx5000-docfeedback@cisco.com

show logging nvram

Use the **show logging nvram** command to display the messages in the NVRAM log.

show logging nvram [**last** *number-lines*]

Syntax Description

last *number-lines*	(Optional) Enters the number of lines to display. The specified number of lines is displayed. Specify from 1 to 100 lines.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the last 20 messages in the NVRAM log:

```
switch# show logging nvram last 20
switch#
```

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 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

Any.

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 allows 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 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
Sat May  3 10:45:49 2008:  Boot Record
--------------------------------------------------------------------------------
Boot Time.........:  Sat May  3 10:45:49 2008
Slot Number.......:  1
Serial Number.....:  FLC12080040
Bios Version......:    v1.0.0(04/01/08)
Firmware Version...:  4.0(0)N1(1) [build 4.0(0)N1(1)]
```

Table 6-1 describes the significant fields shown in the display.

Table 6-1 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.

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

Send comments to nx5000-docfeedback@cisco.com

```
switch# show logging onboard device-version
---------------------------
OBFL Data for
    Module:  1
---------------------------
Device Version Record
-------------------------------------------------------------------------
Timestamp                  Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Sat May  3 10:45:52 2008   ALTOS                 0        2        0
Sat May  3 10:45:52 2008   GATOS                 0        1        0
Sat May  3 10:45:52 2008   GATOS                 1        1        0
Sat May  3 10:45:52 2008   GATOS                 2        1        0
Sat May  3 10:45:52 2008   GATOS                 3        1        0
Sat May  3 10:45:52 2008   GATOS                 4        1        0
Sat May  3 10:45:52 2008   GATOS                 5        1        0
Sat May  3 10:45:52 2008   GATOS                 6        1        0
Sat May  3 10:45:52 2008   GATOS                 7        1        0
Sat May  3 10:45:52 2008   GATOS                 8        1        0
Sat May  3 10:45:52 2008   GATOS                 9        1        0
Sat May  3 10:45:52 2008   GATOS                10        1        0
Sat May  3 10:45:52 2008   GATOS                11        1        0
Sat May  3 10:45:52 2008   GATOS                12        1        0
Sat May  3 10:45:52 2008   GATOS                13        1        0
```

Table 6-2 describes the significant fields shown in the display.

Table 6-2 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
---------------------------
OBFL Data for
    Module:  1
---------------------------

OBFL history records:
--------------------
Mon May 12 03:45:57 2008        : OBFL all logs cleared
Mon May 12 03:56:09 2008        : OBFL environmental-history logging enabled
Mon May 12 03:56:37 2008        : OBFL obfl-log logging to disabled
Mon May 12 03:57:12 2008        : OBFL obfl-log logging enabled
```

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.

Send comments to nx5000-docfeedback@cisco.com

This example shows how to display the OBFL kernel stack trace information:

```
switch# show logging onboard module 2 stack-trace
==================== STACK TRACE ====================
Logging time: Sat Feb 29 19:47:38 2008
watchdog timeout: process swapper (0), jiffies 0x169bb
Stack: c0006e98 c001721c d195f5b4 c0005424 c0005500 c0003e90 c0005a2c c0005a40
c0001a88 c01bf610 c0000394
Call Trace:
print_stack2_buf + 0x50
kernel_thread + 0xb94
klm_cctrl + 0x4554
ppc_irq_dispatch_handler + 0x190
do_IRQ + 0x3c
ret_from_intercept + 0x0
probe_irq_mask + 0x494
probe_irq_mask + 0x4a8
transfer_to_handler + 0x15c
softnet_data + 0x2b0
Registers:
NIP: C0005A20 XER: 00000000 LR: C0005A2C SP: C01AA120 REGS: c01aa070 TRAP: 0500
Tainted: PF
MSR: 00009000 EE: 1 PR: 0 FP: 0 ME: 1 IR/DR: 00
DEAR: C0029B40, ESR: C01F0000
MCSRR0: 00000000, MCSRR1: 00000000, MCAR: 00000000
MCSR: 00000000 MCAR: 00000000 MCPSUMR: 00000000
TASK = c01a8190[0] 'swapper' Last syscall: 120
last math 00000000 last altivec 00000000 last spe 00000000
GPR00: 00000000 C01AA120 C01A8190 00000000 00000032 C8F1DE28 D1010A9F 00000000
GPR08: 0000180F C01FA39C D1010AA3 C01B8D18 24044244 1003A44C 0FFF6700 10049000
GPR16: 0FFAE1B0 0FFFAC90 00000000 00000000 00000000 00000000 00000000 00000001
GPR24: 00000000 00000000 00001160 007FFEAB 007FFE00 C01F0000 C01F0000 00000000
```

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 server

Use the **show logging server** command to display the syslog server configuration.

show logging server

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the syslog server configuration:

```
switch# show logging server
switch#
```

Related Commands

Command	Description
logging server	Configures a remote syslog server.

Send comments to nx5000-docfeedback@cisco.com

show logging session status

Use the **show logging session status** command to display the logging session status.

show logging session status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the logging session status:

```
switch# show logging session status
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show logging status

Use the **show logging status** command to display the logging status.

show logging status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the logging status:

```
switch# show logging status
switch#
```

Send comments to nx5000-docfeedback@cisco.com

show logging timestamp

Use the **show logging timestamp** command to display the logging timestamp configuration.

show logging timestamp

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Any.

Command History

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

Usage Guidelines

None.

Examples

This example shows how to display the logging timestamp configuration:

```
switch# show logging timestamp
switch#
```

Related Commands

Command	Description
logging timestamp	Configures the logging timestamp granularity.

Send comments to nx5000-docfeedback@cisco.com

System Message Logging Facilities

Table 6-3 lists the facilities that you can use in system message logging configuration.

Table 6-3 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	set 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 6-3 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 port-channel 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 6-3 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

Send comments to nx5000-docfeedback@cisco.com

CHAPTER 7

Cisco Nexus 5000 Series Fibre Channel Commands

This chapter describes the Cisco NX-OS Fibre Channel and virtual Fibre Channel 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 in configuration mode. To disable this feature, use the **no** form of the command.

cfs distribute

no cfs distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

CFS distribution is enabled.

Command Modes

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

The following example shows how to disable CFS distribution:

```
switch(config)# no cfs distribute
```

The following 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 in configuration mode. To disable this feature, use the **no** form of the 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

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

The following 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]
```

The following 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 in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv4 mcast-address *ipv4-address*

no cfs ipv4 mcast-address *ipv4-address*

Syntax Description

ipv4-address	Specifies an 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

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 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

The following 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
```

The following 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
```

Send comments to nx5000-docfeedback@cisco.com

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

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 in configuration mode. To disable this feature, use the **no** form of the 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

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

The following 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]
```

The following 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 in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv6 mcast-address *ipv6-address*

no cfs ipv6 mcast-address *ipv6-address*

Syntax Description

ipv6-address	Specifies an 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

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 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

The following 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
```

The following example shows how to revert to the default IPv6 multicast address for CFS distribution over IPv6:

```
switch(config)# no cfs ipv6 ff13::e244:4754
```

Send comments to nx5000-docfeedback@cisco.com

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

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 in the configuration mode. To disable this feature, use the **no** form of this command.

cfs region *region-id*

no cfs region *region-id*

Syntax Description

region-id	Specifies the 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

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

The following example shows how to create a region ID:

```
switch(config)# cfs region 1
```

The following example shows how to assign an application to a region:

```
switch(config)# cfs region 1
switch(config-cfs-region)# ntp, The applications assigned to a region must be registered
with CFS.
```

The following example shows how to remove an application assigned to a region:

```
switch# cfs region 1
switch(config-cfs-region)# no ntp
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
show cfs regions	Displays all configured applications with peers.

Send comments to nx5000-docfeedback@cisco.com

cfs staggered-merge

CFS can merge the data from multiple VSANs. To disable this feature, use the **no** form of this command.

cfs staggered-merge enable

no staggered-merge enable

Syntax Description

enable	Enables the CFS staggered-merge option.

Command Default

Staggered merge is disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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.

Usage Guidelines

None.

Examples

The following 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 in EXEC mode., 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

The following 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 in EXEC mode., clear fcflow stats [aggregated] 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	Specifies the flow index number.

Command Default

None.

Command Modes

EXEC mode.

Command History

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

Examples

The following 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 in EXEC mode., 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

The following 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 FCSM log, use the **clear fcsm log** command in EXEC mode., clear fcsm log

Syntax Description

None.

Command Default

None.

Command Modes

EXEC mode.

Command History

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

Examples

The following 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 in EXEC mode., 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

The following 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 other 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

None.

Examples

The following 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 in EXEC mode., clear fspf counters vsan *vsan-id* [interface *type*]

Syntax Description

vsan	Indicates that the counters are to be cleared for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.
interface *type*	(Optional). 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

The following example clears the FSPF statistics on VSAN 1:

```
switch# clear fspf counters vsan 1
```

The following example clears 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 port-security

To clear the port security information on the switch, use the **clear port-security** command in EXEC mode., clear 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.
session	Clears the port security CFS configuration session and locks.
statistics	Clears the port security counters.
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 1 to 128.
vsan *vsan-id*	Clears entries for a specified VSAN ID. The range is 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 active database is read-only and the **clear port-security database** command can be used when resolving conflicts.

Examples

The following example clears all existing statistics from the port security database for a specified VSAN:

```
switch# clear port-security statistics vsan 1
```

The following example clears learned entries in the active database for a specified interface within a VSAN:

```
switch# clear port-security database auto-learn interface fc2/1 vsan 1
```

The following example clears learned entries in the active database up to for the entire VSAN:

```
switch# clear port-security database auto-learn vsan 1
```

Related Commands

Command	Description
show 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 in EXEC mode., clear rlir {history | recent {interface fc *slot*/*port* | port number *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
port number *port*	Displays the port number for the link incidents
statistics	Clears the RLIR statistics.
vsan *vsan-id*	Clears the RLIR statistics for a 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

None.

Examples

The following example shows how to clear 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 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.

Usage Guidelines

None.

Examples

The following example clears 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 VSAN, use the **clear rscn statistics** command in EXEC mode., clear rscn statistics vsan *vsan-id*

Syntax Description

vsan	Clears the RSCN statistics for a VSAN.
vsan-id	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

None.

Examples

The following example shows how to clear 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 VSAN, use the **clear zone** command in EXEC mode., 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	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

After entering a **clear zone database** command, you need to explicitly enter the **copy running-config startup-config** 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

The following 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 in configuration mode. , device-alias abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following 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 in configuration mode. , device-alias commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit pending changes to the active 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 the command.

device-alias database

no device-alias database

Syntax Description

This command has no other arguments or keywords.

Command Default

Deactivated.

Command Modes

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 submode, 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

The following example shows how to activate a device alias session and enter device alias database configuration submode;

```
switch(config)# device-alias database
switch(config-device-alias-db)#
```

Related Commands

Command	Description
device-alias commit	Commits changes to 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 the command.

device-alias distribute

no device-alias distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

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

The following 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 VSAN, use the **device-alias import fcalias** command. To revert to the default configuration or factory defaults, use the **no** form of the 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 1 to 4093.

Command Default

None.

Command Modes

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 distributed to all other switches in the physical fabric using the **device-alias distribute** command so that new definitions are available everywhere.

Examples

The following 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 the command.

device-alias mode enhanced

no device-alias mode enhanced

Syntax Description

mode enhanced	Specifies enhanced mode.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to device alias enhanced mode:

```
switch(config)# device-alias mode enhanced
```

Related Commands

Command	Description
device-alias database	Enters device alias database configuration submode.
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 the command.

device-alias name *device-name* **pwwn** *pwwn-id*

no device-alias name *device-name*

Syntax Description

device-name	Specifies the device name. Maximum length is 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 submode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following 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 submode.
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 the command.

device-alias rename *device-name1 device-name2*

no device-alias rename *device-name*

Syntax Description

device-name1	Specifies the current device name.
device-name2	Specifies the new device name. Maximum length is 64 characters.

Command Default

None.

Command Modes

Device alias database configuration submode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following 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 submode.
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 VSAN, use the **discover custom-list** command in EXEC mode.**, 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 1 to 4093.
domain *domain-id*	Discovers SCSI targets for the specified domain ID. The range is 1 to 239.

Command Default

None.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

None.

Examples

The following example selectively initiates discovery for the specified VSAN and domain ID:

```
switch# discover custom-list add vsan 1 domain 2
```

The following example deletes 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 in EXEC mode.**, 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 VSAN ID. The range is 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 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.

Usage Guidelines

None.

Examples

The following example shows how to discover local targets assigned to all OSs:

```
switch# discover scsi-target local os all
discovery started
```

The following 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

The following 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...
```

The following 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 QoS setting, use the **fabric profile** command in configuration mode. To restore the default, use the **no** form of the 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

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example sets the fabric to ensure reliable delivery of multicast traffic:

```
switch(config)# fabric profile reliable-multicast
```

The following example sets 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 VSAN, use the **fabric-binding activate** command in configuration mode. To disable this feature, use the **no** form of the 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

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example activates the fabric binding database for the specified VSAN:

```
switch(config)# fabric-binding activate vsan 1
```

The following example deactivates the fabric binding database for the specified VSAN:

```
switch(config)# no fabric-binding activate vsan 10
```

The following example forcefully activates the fabric binding database for the specified VSAN

```
switch(config)# fabric-binding activate vsan 3 force
```

The following example reverts 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 in EXEC mode. **, fabric-binding** database copy vsan *vsan-id*

Syntax Description

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.

If the configured database is empty, this command is not accepted.

Examples

The following example copies 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 VSAN, use the **fabric-binding database diff** command in EXEC mode.**, 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

The following example displays the differences between the active database and the configuration database in VSAN 1:

```
switch# fabric-binding database diff active vsan 1
```

The following example displays 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 VSAN, use the **fabric-binding database vsan** command in configuration mode. To disable the fabric binding, use the **no** form of the 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 hex format.
domain *domain-id*	Specifies the specified domain ID. The domain ID is a number from 1 to 239.

Command Default

None.

Command Modes

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

The following example enters the fabric binding database submode 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
```

The following example deletes a fabric binding database for the specified VSAN:

```
switch(config)# no fabric-binding database vsan 10
```

The following example deletes the sWWN and domain ID of a switch from the configured database list:

```
switch(config)# fabric-binding database vsan 5
switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101
```

Send comments to nx5000-docfeedback@cisco.com

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 VSAN, use the **fabric-binding enable** command. To disable fabric binding, use the **no** form of the command.

fabric-binding enable

no fabric-binding enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

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 participate in the fabric binding.

Examples

The following example enables fabric binding on that switch:

```
switch(config)# fabric-binding enable
```

The following example disables 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

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*	Clones a Fibre Channel alias from the current name to a new name. Maximum length of names is 64 characters.
vsan	The clone Fibre Channel alias is for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

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

The following example shows how to clone a fcalias named 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 the command.

fcalias name *alias name* **vsan** *vsan-id*

no fcalias name *alias name* **vsan** *vsan-id*

Syntax Description

alias-name	The name of the fcalias. Maximum length is 64 characters.
vsan	The fcalias is for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

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

The following 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.

fcalias rename *current-name new-name* **vsan** *vsan-id*

no fcalias rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current fcalias name. The maximum length is 64.
new-name	Specifies the new fcalias name. The maximum length is 64.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following 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 the 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 1 to 4093.
auto-reconfigure	Configures autoreconfigure.
contiguous-allocation	Configures contiguous allocation.
domain *id*	Configures the domain ID and its type. The range is 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*.
fcid	Configures Fibre Channel domain persistent FC IDs.
database	Enters persistent FC IDs submode.
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 1 to 254.
restart	Starts a disruptive or nondisruptive reconfiguration.
disruptive	(Optional) Forces the disruptive fabric reconfiguration.

Command Default

Enabled.

Command Modes

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

The following example shows how to configure a preferred domain ID for VSAN 87:

```
switch(config)# fcdomain domain 3 preferred vsan 87
```

The following example shows how to specify disruptive fabric reconfiguration for VSAN 1:

```
switch(config)# fcdomain restart disruptive vsan 1
```

The following example shows how to enable domain manager fast restart for VSANs 7 through 10:

```
switch(config)# fcdomain optimize fast-restart vsan 7 - 10
```

The following example shows how configure the fabric world wide name (fWWN) for VSAN3:

```
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 and release the lock, use the **fcdomain abort vsan** command. To disable the flushing of cached data, use the **no** form of the command.

fcdomain abort vsan *vsan-id*

no fcdomain abort vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 the command.

fcdomain commit vsan *vsan-id*

no fcdomain commit vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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, us the **no** form of the command.

fcdomain distribute

no fcdomain distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example enables fabric distribution using CFS:

```
switch(config)# fcdomain distribute
```

The following example disables 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 RCF reject flag for a Fibre Channel interface, use the **fcdomain** option. To disable this feature, use the **no** form of the command.

fcdomain rcf-reject vsan *vsan-id*

no fcdomain rcf-reject vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Interface configuration submode

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

The following example shows how to configure the FCIP RCF reject fcdomain feature on a virtual Fibre Channel interface:

```
switch(config)# interface vfc 3/1
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 in configuration mode. To disable the Fibre Channel latency time, use the **no** form of the 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 500 to 60000.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
switch *milliseconds*	Specifies switch latency. The range is 0 to 60000 milliseconds.

Command Default

2000 millisecond network latency.

500 millisecond switch latency.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure the network latency to 5000 milliseconds:

```
switch(config)# fcdroplatency network 5000
```

The following 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 in configuration mode. To disable the counter, use the **no** form of the 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 1 to 2147483647.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
destination-fcid	Enters the destination FCID in hexadecimal format.
source-fcid	Enters the source FCID in hexadecimal format.
netmask	Enters the mask for the source and destination FCID (restricted to 6 hexadecimal characters ranging from 0xff0000 to 0xffffff).

Command Default

None.

Command Modes

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 or each new flow. The number space for flow index is shared between the aggregate flow statistics and the flow statistics.

Examples

The following example enables the aggregated flow counter:

```
switch(config)# fcflow stats aggregated index 1005 vsan 1
```

The following example disables the aggregated flow counter:

```
switch(config)# no fcflow stats aggregated index 1005
```

The following example enables the flow counter for a specific flow:

```
switch(config)# fcflow stats index 1 0x145601 0x5601 0xffffff vsan 1
```

The following example disables 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

Use the **fcid-allocation** command to manually add a FCID to the default area company ID list. Use the **no** form of the command to remove a FCID from the default area company ID list.

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

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 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 exhibiting this behavior. Each HBA is identified by its company ID (also known as Organizational Unique Identifier, or OUI) used in the pWWN during a fabric log in. 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

The following example adds a new company ID to the default area company ID list:

```
switch(config)# fc-id 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 in configuration mode. To disable FCIDs on the switch, use the **no** form of the command.

fcinterop fcid-allocation {**auto** | **flat** | **none**}

no fcinterop fcid-allocation {**auto** | **flat** | **none**}

Syntax Description

auto	Assigns single FCID to compatible HBAs.
flat	Assign single FCID.
none	Assigns FCID range.

Command Default

The default is automatic allocation of FCIDs.

Command Modes

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

The following example sets 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 in configuration mode.

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 VSAN ID. The range is 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

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 in configuration mode.

fcns proxy-port *wwn-id* **vsan** *vsan-id*

no fcns proxy-port *wwn-id* **vsan** *vsan-id*

Syntax Description

wwn-id	Specifies the port WWN, with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

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 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

The following example shows configuring 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 VSAN, use the **fcns reject-duplicate-pwwn vsan** command in configuration mode.

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 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example rejects 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

fcping

To ping an N port, use the **fcping** command in EXEC mode.**, 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. Maximum length is 64 characters.
fcid	The FCID of the destination N port.
fc-port	The port FCID, with the format *0xhhhhhh*.
domain-controller-id	Verifies connection 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 1 to 4093.
count *number*	(Optional) Specifies the number of frames to send. A value of 0 sends forever. The range is 0 to 2147483647.
timeout *value*	(Optional) Specifies the timeout value in seconds. The range is 1 to 10.
usr-priority *priority*	(Optional) Specifies the priority the frame receives in the switch fabric. The range is 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

The following example shows a fcping operation for the FCID of the destination. By default, five frames are sent.

```
switch# fcping fcid 0xd70000 vsan 1
```

The following example shows the setting of 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
```

The following example shows the setting of the timeout value. The default period to wait is 5 seconds. The range is from 1 through 10 seconds.

```
switch# fcping fcid 0xd500b4 vsan 1 timeout 10
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays 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 the command.

fcroute {*fcid* [*network-mask*] **interface** {**fc** *slot*/*port* | **san-port-channel** *port* | **vfc** *vig-num*/*vint-id*} **domain** *domain-id* {**metric** *number* | **remote** | **vsan** *vsan-id*}}

no fcroute {*fcid network-mask* **interface** {**fc** *slot*/*port* | **san-port-channel** *port* | **vfc** *vig-num*/*vint-id*} **domain** *domain-id* {**metric** *number* | **remote** | **vsan** *vsan-id*}}

Syntax Description

fcid	Specifies the FC ID. The format is 0xhhhhhh.
network-mask	Specifies the network mask of the FC ID. The format is 0x0 to 0xffffff.
interface	Specifies an interface.
fc *slot*/*port*	Specifies a Fibre Channel interface.
san-port-channel *port*	Specifies a SAN port channel interface.
vfc *vig-num*/*vint-id*	Specifies a virtual Fibre Channel interface.
domain *domain-id*	Specifies the route for the domain of the next hop switch. The range is 1 to 239.
metric *number*	Specifies the cost of the route. The range is 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 1 to 4093.

Command Default

None.

Command Modes

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

The following example specifies 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
```

The following example specifies the SAN port channel interface and the route for the domain of the next hop switch for VSAN 4:

```
switch(config)# fcroute 0x111211 interface san-port-channel 1 domain 3 vsan 4
```

Send comments to nx5000-docfeedback@cisco.com

The following example specifies 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
```

The following example specifies 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 FCS platform and node-name checking fabric wide, use the **fcs plat-check-global** command in configuration mode. To disable this feature, use the **no** form of the 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

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

```
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 FCS attributes, use the **fcs register** command in configuration mode. To disable this feature, use the **no** form of the command.

fcs register

no fcs register

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 in configuration mode. To remove a virtual device, use the **no** form of the 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 1 to 4093.

Command Default

Disabled.

Command Modes

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

The following example shows how to add to one range of VSANs:

```
switch(config)# fcs virtual-device-add vsan-ranges 2-4
```

The following 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 an 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 the 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) Specifies the 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 **fcsp enable** command.

Examples

The following example turns 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)#
```

The following example reverts to the factory default of auto-passive for the selected interface:

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

The following example changes 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
fcsp enable	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 in configuration mode. This command is only available when the FC-SP feature is enabled. Use the **no** form of the command to revert to factory defaults.

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	Provides the WWN of the device being configured.
password	Configures DHCHAP password for the local switch.
0	(Optional) Specifies a clear text password.
7	(Optional) Specifies a password in encrypted text.
dhgroup	Configures DHCHAP Diffie-Hellman group priority list.
0	(Optional) 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 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) The WWN ID with the format hh:hh:hh:hh:hh:hh:hh:hh.

Command Default

Disabled.

Command Modes

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 **fcsp enable** command.

Using SHA-1 as the hash algorithm may prevent RADIUS or TACACS+ usage.

If you change the DH group configuration, ensure to change it globally for all switches in the fabric.

Examples

The following example enables FC-SP:

```
switch(config)# # fcsp enable
```

Send comments to nx5000-docfeedback@cisco.com

The following example configures the use of only the SHA-1 hash algorithm:

```
switch(config)# fcsp dhchap hash sha1
```

The following example configures the use of only the MD-5 hash algorithm:

```
switch(config)# fcsp dhchap hash md5
```

The following example defines 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
```

The following example reverts 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
```

The following example prioritizes the use of DH group 2, 3, and 4 in the configured order:

```
switch(config)# fcsp dhchap group 2 3 4
```

The following example configures a clear text password for the local switch:

```
switch(config)# fcsp dhchap password 0 mypassword
```

The following example configures 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
```

The following example configures a password entered in an encrypted format for the local switch:

```
switch(config)# fcsp dhchap password 7 sfsfdf
```

Related Commands

Command	Description
fcsp enable	Enable FC-SP.
show fcsp	Displays configured FC-SP information.

Send comments to nx5000-docfeedback@cisco.com

fcsp enable

To enable the Fibre Channel Security Protocol (FC-SP) in a switch, use the **fcsp enable** command in configuration mode. Additional FC-SP commands are available when the FC-SP feature is enabled. To disable FC-SP, use the **no** form of the command.

fcsp enable

no fcsp enable

Syntax Descriptionf

fcsp	Specifies the FC-SP feature in the switch.
enable	Enables the FC-SP feature in this switch.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example enables FC-SP:

```
switch(config)# fcsp enable
```

Related Commands

Command	Description
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 in EXEC mode. Use the **no** form of the command to revert to factory defaults.

fcsp reauthenticate interface { **fc** *slot*/*port* | **vfc** *vig-num*/*vint-id* }

no fcsp reauthenticate interface { **fc** *slot*/*port* | **vfc** *vig-num*/*vint-id* }

Syntax Description

interface	Specifies the interface on which to perform the reauthentication.
interface fc *slot*/*port*	Specifies the Fibre Channel interface by slot and port number.
vfc *vig-num*/*vint-id*	Specifies the virtual Fibre Channel interface by 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.

Usage Guidelines

None.

Examples

The following example configures the FCSP reauthentication on a virtual Fibre Channel interface:

```
switch# fcsp reauthenticate vfc 1/1
```

Related Commands

Command	Description
fcsp enable	Enable FC-SP.
show fcsp	Displays configured FC-SP information.

Send comments to nx5000-docfeedback@cisco.com

fcsp timeout

To configure the timeout value for FC-SP message, use the **fcsp timeout** command in configuration mode. Use the **no** form of the command to revert to factory defaults.

fcsp timeout *timeout-period*

no fcsp timeout *timeout-period*

Syntax Description

timeout-period	Specifies the time out period. The time ranges from 20 to 100 seconds.

Command Default

30 seconds.

Command Modes

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 enter the **fcsp enable** command.

Examples

The following example configures the FCSP timeout value:

```
switch(config)# fcsp enable
switch(config)# fcsp timeout 60
```

Related Commands

Command	Description
fcsp enable	Enable 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 in configuration mode. To revert to the default values, use the **no** form of the 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 5000 to 100000 milliseconds.
e_d_tov *milliseconds*	Specifies the error detect timeout value (ED_TOV). The range is 1000 to 100000 milliseconds, with a default of 2000.
r_a_tov *milliseconds*	Specifies the resolution allocation timeout value (RA_TOV). The range is 5000 to 100000 milliseconds with a default of 10000.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is 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

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

The following 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 in configuration mode.**, fctimer abort**

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following 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 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 in configuration mode. **, fctimer commit**

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following 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 fctimer.
show fctimer	Displays fctimer information.

Send comments to nx5000-docfeedback@cisco.com

fctimer distribute

To enable Cisco Fabric Services (CFS) distribution for Fibre Channel timer (fctimer), use the **fctimer distribute** command. To disable this feature, use the **no** form of the command.

fctimer distribute

no fctimer distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

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

The following example shows how to change the default Fibre Channel timers:

```
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 in EXEC mode**., fctrace** {**device-alias** *aliasname* | **fcid** *fcid* | **pwwn** *pwwn-id*} **vsan** *vsan-id* [**timeout** *seconds*]

Syntax Description

device-alias *aliasname*	Specifies the device alias name. Maximum length is 64 characters.
fcid *fcid*	The FCID of the destination N port, with the format **0x***hhhhhh*
pwwn *pwwn-id*	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 1 to 4093.
timeout *seconds*	Configures the timeout value. The range is 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.

Usage Guidelines

None.

Examples

The following example traces a route to the specified fcid in VSAN 1:

```
switch# fctrace fcid 0x660000 vsan 1
```

The following example traces 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 FDMI updates, use the **fdmi suppress-updates** command in configuration mode.**, fdmi suppress-updates vsan** *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

By default, FDMI updates are not suppressed.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example suppresses FDMI updates in VSAN 1:

```
switch# fdmi suppress-updates vsan 1
```

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 the command.

feature fcoe

no feature fcoe

Syntax Description

This command has no arguments or keywords.

Command Default

FCoE is disabled.

Command Modes

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
```

Send comments to nx5000-docfeedback@cisco.com

fspf config

To configure an FSPF feature for an entire VSAN, use the **fspf config** command in configuration mode. This command enters FSPF configuration mode, which includes four commands (each with a **no** form).

To delete FSPF configuration for the entire VSAN, use the **no** form of the 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 1 to 4093.
min-ls-arrival *ls-arrival-time*	This command specifies the minimum time before a new link state update for a domain will be accepted by switch. The parameter *ls-arrival-time* is an integer specifying time in milliseconds. The range is 0 to 65535.
min-ls-interval *ls-interval-time*	This command specifies the minimum time before a new link state update for a domain will be generated by the switch. The parameter *ls-interval-time* is an integer specifying time in milliseconds. The range is 0 to 65535.
region *region-id*	This command specifies the autonomous region to which the switch belongs. The backbone region has *region-id*=0. The parameter *region-id* is an unsigned integer value ranging from 0 to 255.
spf	This command specifies parameters related to 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. The parameter *spf-holdtime* is an integer specifying time in milliseconds. The range is 0 to 65535.
static	Forces static SPF computation.

Command Default

In FSPF configuration mode, the default is dynamic SPF computation.

If configuring spf hold-time, the default value for FSPF is 0.

If configuring min-ls-arrival, the default value for FSPF is 1000 milliseconds.

If configuring min-ls-interval, the default value for FSPF is 5000 milliseconds.

Command Modes

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 VSAN. In FSPF configuration mode, the commands configure FSPF for this VSAN .

Examples

The following example configures static SPF computation in VSAN 1 and deletes the FSPF configuration in VSAN 3:

```
switch(config)# fspf config vsan 1
switch(fspf-config)# spf static
switch(fspf-config)# exit
switch(config)#
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 specified VSAN

Send comments to nx5000-docfeedback@cisco.com

fspf cost

To configure FSPF link cost for an FCIP interface, use the **fspf cost** command. To revert to the default value, use the **no** form of the command.

fspf cost *link-cost* **vsan** *vsan-id*

no fspf cost *link-cost* **vsan** *vsan-id*

Syntax Description

link-cost	Enters FSPF link cost in seconds. The range is 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 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 submode.

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

The following example configures 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 the command.

fspf dead-interval *seconds* **vsan** *vsan-id*

no fspf dead-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	Specifies the FSPF dead interval in seconds. The range is 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

80 seconds.

Command Modes

Interface configuration submode.

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

The following example configures 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 FSPF for a VSAN, use the **fspf enable** command in configuration mode. To disable FSPF routing protocols, use the **no** form of the command.

fspf enable vsan *vsan-id*

no fspf enable vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

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

The following example enables FSPF in VSAN 5 and disables FSPF in VSAN 7:

```
switch## configure
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 the 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 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

20 seconds.

Command Modes

Interface configuration submode.

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

The following example configures 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 FSPF protocol for selected interfaces, use the **fspf passive** command. To revert to the default state, use the **no** form of the command.

fspf passive vsan *vsan-id*

no fspf passive vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

FSPF is enabled.

Command Modes

Interface configuration submode.

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

The following example disables 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 the command.

fspf retransmit-interval *seconds* **vsan** *vsan-id*

no spf retransmit-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	Specifies FSPF retransmit interval in seconds. The range is 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

5 seconds.

Command Modes

Interface configuration submode.

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

The following example specifies 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 in configuration mode. To disable in-order delivery, use the **no** form of the command.

in-order-guarantee [**vsan** *vsan-id*]

no in-order-guarantee [**vsan** *vsan-id*] [**,**] [-]

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 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

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

The following example shows how to enable in-order delivery for the entire switch:

```
switch(config) # in-order-guarantee
```

The following example shows how to disable in-order delivery for the entire switch:

```
switch(config)# no in-order-guarantee
```

The following example shows how to enable in-order delivery for a specific VSAN:

```
switch(config)# in-order-guarantee vsan 3452
```

The following 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 in configuration mode. The **interface fc** command enters interface configuration mode, which includes five commands (each with a **no** form).

To revert to defaults, use the **no** form of the 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	Specifies a slot number and port number.
channel-group	Adds to or removes from a Port Channel.
group-id	Specifies a Port Channel group number from 1 to 128.
force	Forcefully adds a port.
auto	Enables autocreation of port channels.
fcdomain	Enters the interface submode.
rcf-reject	Configures the rcf-reject flag.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
fspf	Configures FSPF parameters.
cost *link-cost*	Configures FSPF link cost. The range is 1 to 65535.
dead-interval *seconds*	Configures FSPF dead interval in seconds. The range is 2 to 65535.
hello-interval *seconds*	Configures FSPF hello-interval. The range is 1 to 65535.
passive	Enables or disables FSPF on the interface.
retransmit-interval *seconds*	Configures FSPF retransmit interface in seconds. The range is 1 to 65535.

Command Default

Disabled.

Command Modes

Configuration mode.

Send comments to nx5000-docfeedback@cisco.com

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*space***fc1/1***space-space***5***space*,*space***fc2/5***space-space***7**

Refer to the *Cisco Nexus 5000 Series CLI Configuration Guide* for information on port number allocation.

Use the **no shutdown** command to enable the interface.

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

The following example configures ports 1 to 4 in Fibre Channel interface 3:

```
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# int fc3/1 - 4
```

The following example enables the Fibre Channel interface in port 1 of slot 3:

```
switch(config)# interface fc3/1
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 in configuration mode. The **interface san-port-channel** command enters interface configuration mode, which includes six commands (each with a **no** form).

To revert to defaults, use the **no** form of the 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	Specifies a port number.
description *line*	Enters a line of text to describe the interface.
shutdown	Changes the interface state to administrative down.
force	Forces the interface state to administrative down.
switchport	Enters configuration parameters for the SAN port channel .

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

Use the **no shutdown** command to enable the interface.

Examples

The following example configures SAN port channel interface 3:

```
switch(config)# interface san-port-channel 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

interface vig

To configure a virtual interface group (VIG) on a Cisco Nexus 5000 Series switch, use the **interface vig** command in configuration mode. The **interface vig** command enters interface configuration mode, which provides one command (and its **no** form).

To revert to defaults, use the **no** form of the command.

interface vig *vig-num*
  bind interface ethernet *slot/port*

no interface vig *vig-num*
  no bind interface ethernet *slot/port*

Syntax Description

vig-num	Specifies the virtual interface group number.
bind interface	Specifies the interface to associate with this VIG.
ethernet *slot/port*	Specifies the slot and port of physical Ethernet interface.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

This command creates a virtual Interface Group (if it does not already exist) and enters interface configuration mode for the specified VIG.

Examples

The following example creates virtual interface group 3 and associates it with a physical Ethernet interface:

```
switch(config)# interface vig 3
switch(config-if)# bind interface ethernet 1/15
```

Related Commands

Command	Description
show vig	Displays the configuration for the specified VIG.

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 in configuration mode. To revert to defaults, use the **no** form of the command.

interface vfc *vig-num/vint-id*
description *line*
shutdown [**force**]
switchport {**mode F**}

no interface vfc *vig-num/vint-id*
no description
no shutdown
no switchport mode

Syntax Description

vig-num/vint-id	Specifies a VIG number and a virtual interface ID.
description *line*	Enters a line of text to describe the interface.
shutdown	Changes the interface state to administrative down.
switchport mode F	Specifies the mode of the virtual Fibre Channel interface.

Command Default

Disabled.

Command Modes

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 vfc1/1,vfc2/1

Refer to the *Cisco Nexus 5000 Series CLI Configuration Guide* for information on port number allocation.

Use the **no shutdown** command to enable the interface.

Examples

The following example configures port 1 in virtual Fibre Channel interface 3:

```
switch(config)# interface vfc3/1
```

The following example enables the virtual Fibre Channel interface:

```
switch(config)# interface vfc3/1
switch(config-if)# no shutdown
```

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

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
lldp (Interface)	Configures the LLDP feature on an interface.
show lldp	Displays the 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.

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

Command	Description
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 in configuration mode.**, logging abort**

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to discard 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 **in configuration mode., logging commit**

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 the command.

logging distribute

no logging distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

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

The following 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 submode)

To add a member name to a Fibre Channel alias on a VSAN, use the **member** command in fcalias configuration submode. To remove a member name from a Fibre Channel alias, use the **no** form of the 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. Maximum length is 64 characters.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
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.
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.
port-number *port-number*	Specifies a port number in the range of 0 to 255.
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 submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to add a member to an alias called samplealias:

```
switch(config)# fcalias name samplealias
```

Send comments to nx5000-docfeedback@cisco.com

The following example defines a Fibre Channel interface for the member:

```
switch(switch(config-fcalias)# member interface fc3/1
```

The following 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 submode)

To add a member name to a Fibre Channel zone, use the **member** command in zone configuration submode. To remove a member name from a zone, use the **no** form of the 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. Maximum length is 64 characters.
lun *lun-id*	Specifies the member LUN ID. The format is *0***x***hhhh*[**:***hhhh*[**:***hhhh*[**:***hhhh*]]], where *h* is a hexadecimal digit.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
alias-name	The name of the fcalias. Maximum length is 64 characters.
port-number *port*	Specifies the member port number. The range is 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.
swwn *swwn-id*	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

This command can be used in both zone configuration submode and zoneset-zone configuration submode.

Command Modes

Zone set zone configuration submode and zoneset-zone configuration submode.

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

The following 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
```

The following example shows how to add a zone to a zoneset called Zoneset1 on VSAN 1:

```
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)# member fcid 0x111112
```

The following 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
```

The following 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 submode)	Used to specify a name for a zone set.
zone name (zone set configuration submode)	Configures a zone in a zoneset.
show zoneset	Displays zone set information.

Send comments to nx5000-docfeedback@cisco.com

member (zoneset configuration submode)

To configure zone set members, use the **member** command in zone set configuration submode. To remove a zone set member, use the **no** form of the command.

member *member-name*

no member *member-name*

Syntax Description

member-name	Specifies the member name. Maximum length is 64 characters.

Command Default

None.

Command Modes

Zone set configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following 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

npiv enable

To enable N Port Identifier Virtualization (NPIV) for all VSANs on a switch, use the **npiv enable** command in configuration mode. To disable NPIV, use the **no** form of the command.

npiv enable

no npiv enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

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

The following example enables NPIV for all VSANs on the switch:

```
switch(config)# npiv enable
```

The following example disables NPIV for all VSANs on the switch:

```
switch(config)# no npiv enable
```

Related Commands

Command	Description
show interface	Displays interface configurations.

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 in configuration mode. To disable this feature, use the **no** form of the command.

npv auto-load-balance disruptive

no npv auto-load-balance disruptive

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

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

The following example shows how to enable disruptive load-balancing:

```
switch# config
switch(config)# npv auto-load-balance disruptive
```

Related Commands

Command	Description
npv enable	Enables NPV mode.
show npv status	Displays the NPV current status.

Send comments to nx5000-docfeedback@cisco.com

npv enable

To enable N Port Virtualization (NPV) mode, use the **npv enable** command in configuration mode. To disable this feature, use the **no** form of the command.

npv enable

no npv enable

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

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

The following example shows how to enable NPV mode:

```
switch# config
switch(config)# npv enable
```

Related Commands

Command	Description
show npv status	Displays the NPV current status.

Send comments to nx5000-docfeedback@cisco.com

port-security

To configure port security features and reject intrusion attempts, use the **port-security** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

port-security {**activate vsan** *vsan-id* [**force** | **no-auto-learn**] | **auto-learn vsan** *vsan-id* | **database vsan** *vsan-id* }

no 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.
auto-learn	Enables auto-learning for the specified VSAN.
database	Enters the port security database configuration mode for the specified VSAN.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
force	(Optional) Forces the database activation.
no-auto-learn	(Optional) Disables the auto-learning feature for the port security database.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

When you activate the port security feature, the **auto-learn** option is also automatically enabled. You can choose to activate the port-security feature and disable auto-learning using the **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.

Examples

The following example activates the port security database for the specified VSAN, and automatically enables auto-learning:

```
switch(config)# port-security activate vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

The following example deactivates the port security database for the specified VSAN, and automatically disables auto-learning:

```
switch(config)# no port-security activate vsan 1
```

The following example disables the auto-learning feature for the port security database in VSAN 1:

```
switch(config)# port-security activate vsan 1 no-auto-learn
```

The following example enables 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)# port-security auto-learn vsan 1
```

The following example disables auto-learning and stops the switch from learning about new devices accessing the switch:

```
switch(config)# no port-security auto-learn vsan 1
```

The following example enters the port security database mode for the specified VSAN:

```
switch(config)# port-security database vsan 1
switch(config-port-security)#
```

The following example forces the VSAN 1 port security database to activate even if there are conflicts:

```
switch(config)# port-security activate vsan 1 force
```

Related Commands

Command	Description
show port-security database	Displays configured port security information.

Send comments to nx5000-docfeedback@cisco.com

port-security abort

To discard the port security Cisco Fabric Services (CFS) distribution session in progress, use the **port-security abort** command **in configuration mode., port-security abort** vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to discard a port security CFS distribution session in progress:

```
switch(config)# port-security abort vsan 33
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

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 **port-security commit** command in configuration mode**., port-security commit** vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active port security configuration:

```
switch(config)# port-security commit vsan 13
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

port-security database

To copy the port security database or to view the difference within the port security database, use the **port-security database** command in EXEC mode.**, 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 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

If the active database is empty, the port-security database is empty.

Use the **port-security database diff active** command to resolve conflicts.

Examples

The following example copies the active to the configured database:

```
switch# port-security database copy vsan 1
```

The following example provides the differences between the active database and the configuration database:

```
switch# port-security database diff active vsan 1
```

The following example provides information on the differences between the configuration database and the active database:

```
switch# port-security database diff config vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
port-security database	Copies and provides information on the differences within the port security database.
show port-security database	Displays configured port security information.

Send comments to nx5000-docfeedback@cisco.com

port-security distribute

To enable Cisco Fabric Services (CFS) distribution for port security, use the **port-security distribute** command. To disable this feature, use the **no** form of the command.

port-security distribute

no port-security distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

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 **port-security commit** command.

Examples

The following example shows how to distribute the port security configuration to the fabric:

```
switch(config)# port-security distribute
```

Related Commands

Command	Description
port-security commit	Commits the port security configuration changes to the active configuration.
show port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

port-security enable

To enable port security, use the **port-security enable** command in configuration mode. To disable port security, use the **no** form of the command.

port-security enable

no port-security enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

Entering the **port-security enable** command enables the other commands that are used to configure port security.

Examples

The following example shows how to enable port security:

```
switch(config)# port-security enable
```

The following example shows how to disable port security:

```
switch(config)# no port-security enable
```

Related Commands

Command	Description
show port-security	Displays port security information.

Send comments to nx5000-docfeedback@cisco.com

port-track enable

To enable port tracking for indirect errors, use the **port-track enable** command in configuration mode. To disable this feature, use the **no** form of the command.

port-track enable

no port-track enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

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

The following example shows how to enable port tracking:

```
switch(config)# port-track enable
```

The following example shows how to disable port tracking:

```
switch(config)# no port-track enable
```

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

port-track force-shut

To force a shutdown of a tracked port, use the **port-track force-shut** command in interface configuration submode. To reenable the port tracking, use the **no** form of the command.

port-track force-shut

no port-track force-shut

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode.

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 using the **no port-track force-shut** command.

Examples

The following 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
port-track enable	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 in interface configuration submode. To disable this feature, use the **no** form of the 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 1 to 128.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Interface configuration submode.

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

The following 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
port-track enable	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 in EXEC mode., 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 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

None.

Examples

The following example shows how to purge all dynamic, unused FCIDs in VSAN 4:

```
switch# purge fcdomain fcid vsan 4
```

The following 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 in configuration mode. To remove a preferred host, use the **no** form of the 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 1 to 4093.

Command Default

By default, the switch sends RLIR frames to one of the hosts in the VSAN with the register function set to “conditionally receive” if no hosts have the register function set to “always receive.”

Command Modes

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

The following example specifies FC ID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch(config)# rlir preferred-cond fcid 0x654321 vsan 2
```

The following example removes FC ID 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 in configuration mode.**, 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

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example configures RSCNs in multi-PID format:

```
switch(config)# rscn multi-pid vsan 1
```

Related Commands

Command	Description
show rscn src-table	Displays 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 VSAN, use the **rscn abort** command in configuration mode. To reverse the cancellation, use the **no** form of the 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 cancelled. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example cancels 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 in configuration mode. To discard a pending RSCN configuration, use the **no** form of the 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

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

The following example commits 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 in configuration mode. To disable the distribution, use the **no** form of the command.

rscn distribute

no rscn distribute

Syntax Description

This command has no arguments or keywords.

Command Default

RSCN timer distribution is disabled.

Command Modes

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 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

The following example enables 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 VSAN, use the **rscn event-tov** command in configuration mode. To cancel the event timeout value and restore the default value, use the **no** form of the command.

rscn event-tov *timeout* **vsan** *vsan-id*

no rscn event-tov *timeout* **vsan** *vsan-id*

Syntax Description

timeout	Specifies an event timeout value in milliseconds. The range is 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

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

The following example configures 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 in EXEC mode., san-port-channel *port-channel-id* persistent

Syntax Description

port-channel-id	Specifies the port channel ID. The range is 1 to 128.
persistent	

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 member ports properties change to those of a user-created channel group. The channel mode remains active.

Examples

The following 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 in configuration mode. To remove SCSI target discovery, use the **no** form of the 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*	Specifies a VSAN ID. The range is 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

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 the command.

Examples

The following example configures SCSI target auto-polling discovery for VSAN 1:

```
switch(config)# scsi-target auto-poll vsan 1
```

The following example removes SCSI target auto-polling discovery for VSAN 1:

```
switch(config)# no scsi-target auto-poll vsan 1
```

The following example configures a SCSI target discovery:

```
switch(config)# scsi-target discovery
```

The following example configures SCSI target ns-polling discovery for VSAN 1:

```
switch(config)# scsi-target ns-poll vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

The following example removes SCSI target ns-polling discovery for VSAN 1:

```
switch(config)# no scsi-target ns-poll vsan 1
```

The following example configures SCSI target on-demand discovery for VSAN 1:

```
switch(config)# scsi-target on-demand vsan 1
```

The following example removes 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

switchport

To configure a switch port parameter on a Fibre Channel or virtual Fibre Channel interface, use the **switchport** command in interface configuration submode. To discard the configuration, use the **no** form of the command.

Fibre Channel Interface:

switchport { **encap eisl** |
fcrxbbcredit {*credit* [**mode E** | **F**] | **default** | } |
mode {**auto** | **E** | **F** | **SD** |} |
speed {**1000** | **2000** | **4000** | **auto** [**max 2000**]} |
trunk {**allowed vsan** {[**add**] *vsan-id* | **all**} | **mode** {**auto** | **off** | **on**}}}

no switchport { **encap eisl** | **fcrxbbcredit**| **fcrxbufsize** *size* | **mode** | **rate** | **speed** | **trunk allowed vsan** [[**add**] *vsan-id* | **all**]}

Virtual Fibre Channel Interface:

switchport mode F

Syntax Description

encap eisl	Configures extended ISL (EISL) encapsulation for the interface.
fcrxbbcredit	Configures receive BB_credit for the port.
credit	Specifies receive BB_credit. The range is 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.
auto	Configures autosense mode.
E	Configures E port mode.
F	Configures F port 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.
auto	Configures autosense speed.
max 2000	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	Specifies the VSAN ID. The range is 1 to 4093.

Send comments to nx5000-docfeedback@cisco.com

all	Adds all the VSANs to allowed VSAN list.
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 submode.

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*space***fc2/1***space*-*space***2***space*,*space***fc3/2***space*-*space***4**

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

The following example configures switch port parameters for a Fibre Channel interface:

```
switch(config)# interface fc 2/3
switch(config-if)# switchport description techdocsSample
switch(config-if)# switchport mode E
switch(config-if)# switchport trunk mode auto
switch(config-if)# switchport trunk allowed vsan all
```

Send comments to nx5000-docfeedback@cisco.com

```
switch(config-if)# switchport trunk allowed vsan 3
switch(config-if)# switchport trunk allowed vsan add 2
switch(config-if)# switchport encap eisl
switch(config-if)# switchport fcrxbbcredit 20
```

The following example configures the mode of a virtual Fibre Channel interface:

```
switch(config)# interface vfc 2/1
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 the 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 submode.

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

The following 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
```

The following example shows how to allow the detection of bit error events from disabling the interface:

Send comments to nx5000-docfeedback@cisco.com

```
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 in configuration mode. To disable port attributes, use the **no** form of the 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

Configuration mode.

Command History

Release	Modification
4.0	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

The following example shows how to configure port shutdown:

```
switch(config)# system default switchport shutdown
```

The following example shows how to configure the trunk mode:

```
switch(config)# system default switchport trunkmode 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 in configuration mode. To revert to the defaults, use the **no** form of the 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

Configuration mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command defines the default values for the default zone for all 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 in conjunction 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

The following example sets the default zone to use the default values:

```
switch(config)# system default zone default-zone permit
```

The following example restores 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 in configuration mode. To revert to the defaults, use the **no** form of the 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

Configuration mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command distributes the default values for the default zone to all 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 in conjunction 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

The following example distributes default values to the full zone set:

```
switch(config)# system default zone distribute full
```

The following example distributes 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 in configuration mode. To disable this feature, use the **no** form of the command.

trunk protocol enable

no trunk protocol enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

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 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

The following example shows how to disable the trunk protocol feature:

```
switch(config)# no trunk protocol enable
```

The following 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 database

To create multiple fabrics sharing the same physical infrastructure, assign ports to VSANs, turn on or off interop mode, load balance either per originator exchange or by source-destination ID, and enter VSAN database submode, use the **vsan database** command. To remove a configuration, use the **no** command in VSAN database submode.

vsan database
vsan *vsan-id*
[**interface** {**fc** *slot/port* | **san-port-channel** *port* | **vfc** *vig-num/vint-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**}]]

vsan database
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 1 to 4093.
interface fc *slot/port*	(Optional) Specifies the Fibre Channel interface by slot and port number on the switch.
san-port-channel *portchannel-number.subinterface-number*	Configures the SAN port channel interface specified by the SAN port channel number followed by a dot (.) indicator and the subinterface number.
interop	Turns on interoperability mode.
mode	Specifies the interop mode. The range is 1 to 4.
loadbalancing	Configures 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. Maximum length is 32 characters.
suspend	Suspends the VSAN.

Command Default

None.

Command Modes

Configuration mode.

Send comments to nx5000-docfeedback@cisco.com

Command History

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

Usage Guidelines

To use this command, change to the VSAN database submode.

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

The following 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-db)#
switch-config-db# vsan 2
switch(config-vsan-db)# vsan 2 name TechDoc
updated vsan 2
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
switch#
```

The following example shows how to suspend a VSAN and enable Interop mode 4:

```
switch# config t
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 remove interface fc2/1 from VSAN 7:

Send comments to nx5000-docfeedback@cisco.com

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interface fc2/1
switch(config-vsan-db)#
```

Related Commands

Command	Description
vsan wwn	Configures a WWN for a suspended VSAN that has Interop mode 4 enabled.

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

secondary-mac *wwn-id*	The secondary MAC address with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
range *address-range*	The range for the specified WWN. The only valid value is 64.

Command Modes

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, refer to the *Cisco Nexus 5000 Series CLI Configuration Guide*.

Examples

The following example allocates a secondary range of MAC addresses:

```
switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
From now on WWN allocation would be based on new MACs.
Are you sure? (yes/no) yes
```

Send comments to nx5000-docfeedback@cisco.com

wwn vsan

To configure a WWN for a suspended VSAN that has interop mode 4 enabled, use the **wwn vsan** command in configuration mode. To discard the configuration, use the **no** form of the command.

wwn vsan *vsan-id* **vsan-wwn** *wwn*

no wwn vsan *vsan-id* **vsan-wwn** *wwn*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 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

Configuration submode.

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

The following 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
WWN can be configured for vsan in suspended state only
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
switch(config)#
```

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, and load balances either per originator exchange or source-destination ID.

Send comments to nx5000-docfeedback@cisco.com

zone clone

To clone a zone name, use the **zone clone** command in configuration mode. , zone clone *current-zone-name new-zone-name* vsan *vsan-id*

Syntax Description

current-zone-name *new-zone-name*	Clones a zone attribute group from the current name to a new name. Maximum length of names is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

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

The following example creates a clone of the original zone group named 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 VSAN, use the **zone commit** command in configuration mode. To negate the command, use the **no** form of the 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 1 to 4093.
force	(Optional) Forces the commit.

Command Default

None.

Command Modes

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

The following example commits 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 VSAN, use the **zone compact** command., zone compact vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

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

The following 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 in EXEC mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

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.
vsan *vsan-id*	Configures to copy active zone set on a VSAN to full zone set. The ID of the VSAN is from 1 to 4093.
full-zoneset	Copies the active zone set to the full-zone set.
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 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.
slot0:	Copies the active zone set to a location in the slot0: directory.
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.

Usage Guidelines

None.

Examples

The following example copies the active zone set to the full zone set:

```
switch# zone copy active-zoneset full-zoneset vsan 1
```

The following example copies 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-zon**e command in configuration mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

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 VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

All default zones are permitted access.

Command Modes

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

The following example permits 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 in configuration mode. To disable this feature, use the **no** form of the 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 1 to 4093.

Command Default

Disabled.

Command Modes

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 ISLs between the switches become isolated.

Examples

The following example shows how to set 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 VSAN, use the **zone mode enhanced** command in configuration mode. To disable this feature, use the **no** form of the 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 1 to 4093.

Command Default

Disabled.

Command Modes

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

The following 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 in configuration mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

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	Specifies the name of the zone. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

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 submode.

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

The following example configures 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
```

The following example configures 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 submode)

To configure a zone in a zone set, use the **zone name** command in zone set configuration submode. To delete the zone from the zone set, use the **no** form of the command.

zone name *zone-name*

no zone name *zone-name*

Syntax Description

zone-name	Specifies the name of the zone. Maximum length is 64 characters.

Command Default

None.

Command Modes

Zone set configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example configure a zone in a zone set:

```
switch(config)# zoneset name Sample vsan 1
switch(config-zoneset)# zone name MyZone
```

The following example deletes a zone from a zone set:

```
switch(config-zoneset)# no zone name Zone2
```

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 in configuration mode., zone rename *current-name* *new-name* vsan *vsan-id*

Syntax Description

current-name	Specifies the current fcalias name. Maximum length is 64 characters.
new-name	Specifies the new fcalias name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following 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 in configuration mode. To negate the command or revert to the factory defaults, use the **no** form of the 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
clone *zoneset-currentName zoneset-cloneName*	Clones a zone set from the current name to a new name. Maximum length of names is 64 characters.
name *zoneset-name*	(Optional) Specifies a name for a zone set. Maximum length is 64 characters.
distribute full	Enables zone set propagation.
vsan *vsan-id*	Activates a zone set on the specified VSAN. The range is 1 to 4093.
rename	Renames a zone set.
current-name	Specifies the current fcalias name.
new-name	Specifies the new fcalias name.

Command Default

None.

Command Modes

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

The following example activates a zone set named zSet1 in VSAN 333:

```
switch(config)# zoneset activate name zSet1 vsan 333
```

The following example clones a zone set named zSet1 into a new zoneset named zSetClone in VSAN 45:

```
switch(config)# zoneset clone existing zSet1 zSetClone vsan 45
```

The following example distributes 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 in EXEC mode., 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 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*	(Optional) Configures a Fibre Channel interface for the specified slot number and port number.
san-port-channel *port-number*	Specifies 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

The following example imports the zone set database from the adjacent switch connected through the VSAN 2 interface:

```
switch# zoneset import interface fc2/3 vsan 2
```

The following example exports the zone set database to the adjacent switch connected through VSAN 5:

```
switch# zoneset export vsan 5
```

The following example distributes the zone set in VSAN 333:

```
switch# zoneset distribute vsan 333
```

Send comments to nx5000-docfeedback@cisco.com

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 8

Cisco Nexus 5000 Series Fibre Channel Show Commands

This chapter describes the Cisco NX-OS Fibre Channel 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. Maximum length is 64 characters.
lock	Displays the state of application logical or physical locks.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is 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	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display CFS physical peer information for all applications:

```
switch# show cfs peers
```

The following example shows how to display CFS information for all applications on the switch:

```
switch# show cfs application
```

Note 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.

The following example shows how to display CFS information for the device alias application:

```
switch# show cfs application name device-alias
```

Send comments to nx5000-docfeedback@cisco.com

The following example shows how to display CFS merge operation information for the device alias application:

```
switch# show cfs merge status device-alias
```

The following example shows whether or not CFS distribution is enabled:

```
switch# show cfs status
```

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 other keywords or arguments.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The **show debug npv** command is available only when the switch is in NPV mode.

Examples

The following example shows 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	
name *device-name*	Displays device name database information for a specific device name.
pending	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*:*hh*, where *h* is a hexadecimal number.
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	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

The following example shows how to display the contents of the device alias database:

```
switch# show device-alias database
```

The following example shows how to display all global fcaliases and all VSAN dependent fcaliases:

```
switch# show device-alias name efg
```

The following 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 in EXEC mode.**, 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 VSAN ID. The range is 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 1 to 100.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured fabric binding database information:

```
switch# show fabric-binding database
```

The following example displays active fabric binding information:

```
switch# show fabric-binding database active
```

The following example displays active VSAN-specific fabric binding information:

```
switch# show fabric-binding database active vsan 61
```

The following example displays configured VSAN-specific fabric binding information:

```
switch# show fabric-binding database vsan 4
```

The following example displays fabric binding statistics:

```
switch# show fabric-binding statistics
```

The following example displays fabric binding status for each VSAN:

Send comments to nx5000-docfeedback@cisco.com

```
switch# show fabric-binding status
```

The following example displays EFMD statistics:

```
switch# show fabric-binding efmd statistics
```

The following example displays EFMD statistics for a specified VSAN:

```
switch# show fabric-binding efmd statistics vsan 4
```

The following example displays fabric binding violations:

```
switch# show fabric-binding violations
```

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	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 FC2 VSAN table.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FC2 active socket information:

```
switch# show fc2 socket
```

The following example displays FC2 socket binding information:

```
switch# show fc2 bind
```

The following example displays FC2 local N port information:

```
switch# show fc2 nport
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays FC2 PLOGI session information:

```
switch# show fc2 plogi
```

The following example displays FC2 physical port information:

```
switch# show fc2 port
```

The following example displays FC2 local N port PLOGI notifications for each socket:

```
switch# show fc2 socknotify
```

The following example displays FC2 local N ports for each socket:

```
switch# show fc2 socknport
...
```

The following example displays FC2 VSAN table:

```
switch# show fc2 vsan
....
```

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 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	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

The following example displays 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, 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).
pending	(Optional) Displays the pending configuration.
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.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
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 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	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.

Examples

The following example displays the fcdomain information for VSAN 1:

```
switch# show fcdomain vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays 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 8-1 describes the significant fields shown in the **show fcdomain domain-list** command output.

Table 8-1 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.

The following example displays the allowed domain ID lists:

```
switch# show fcdomain allowed vsan 1
```

The following example shows the status of CFS distribution for allowed domain ID lists:

```
switch# show fcdomain status
```

The following example displays pending configuration changes:

```
switch# show fcdomain pending vsan 10
```

The following example displays the differences between the pending configuration and the current configuration:

```
switch# show fcdomain pending-diff vsan 10
```

The following example displays 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) Network latency in milliseconds.
switch	(Optional) Switch latency in milliseconds.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the configured Fibre Channel latency parameters:

```
switch# show fcdroplatency
```

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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays aggregated fcflow details:

```
switch# show fcflow stats aggregated
```

The following example displays fcflow details:

```
switch# show fcflow stats
```

The following example displays fcflow index usage:

```
switch# show fcflow stats usage
```

Send comments to nx5000-docfeedback@cisco.com

show fcid-allocation

Use the **show fcid allocation** command to display the Fibre Channel area list of company IDs., show fcid-allocation area | company-id-from-wwn *wwn* [*company-id*]

Syntax Description

area	Selects the auto area list of company IDs.
company-id-from-wwn *wwn*	Selects company ID from the specified world wide name (WWN).
company-id	(Optional) Selects the individual company ID (also know as Organizational Unit Identifier, or OUI) to display.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0	New command

Examples

The following example shows 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.
switch#
```

Table 8-2 describes the significant fields shown in the display.

Table 8-2 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

show fcns database

To display the results of the discovery, or to display the name server database for a specified 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 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
1.2(2)	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

The following example displays the contents of the FCNS database:

```
switch# show fcns database
```

The following example displays the detailed contents of the FCNS database:

```
switch# show fcns database detail
```

The following example displays the management VSAN (VSAN 2):

```
switch# show fcns database vsan 2
```

The following example displays the database for all configured VSANs:

```
switch# show fcns database
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands

Command	Description
fcns	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 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 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays statistical information for a specified VSAN:

```
switch# show fcns statistics
```

Send comments to nx5000-docfeedback@cisco.com

show fcoe

To display the status of Fibre Channel over Ethernet (FCoE) on the switch, use the **show fcoe** command.**, show fcoe**

Syntax Description

This command has no other keywords or arguments.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the FCoE status:

```
switch# show fcoe
```

Send comments to nx5000-docfeedback@cisco.com

show fcroute

Use the **show fcroute** command to view specific information about existing Fibre Channel and FSPF configurations., 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 FC route preference.
label	Displays label routes.
label	(Optional) Displays 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) Specifies the Fibre Channel ID.
summary	Displays the FC routes summary.
unicast	Displays FC unicast routes.
host	Displays unicast routes for the specified host.
fc-mask	Displays unicast routes for hosts that match the range of FC IDs that is specified by the mask.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	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

The following example displays administrative distance:

```
switch# show fcroute distance
...
```

The following example displays multicast routing information:

```
switch# show fcroute multicast
...
```

The following example displays FCID information for a specified VSAN:

```
switch# show fcroute multicast vsan 3
```

The following example displays FCID and interface information for a specified VSAN:

```
switch# show fcroute multicast 0xffffff vsan 2
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays unicast routing information:

```
switch# show fcroute unicast
```

The following example displays unicast routing information for a specified VSAN:

```
switch# show fcroute unicast vsan 4
```

The following example displays unicast routing information for a specified FCID:

```
switch# show fcroute unicast 0x040101 0xffffff vsan 4
```

The following example displays route database information:

```
switch# show fcroute summary
```

The following example displays route database information for a specified VSAN:

```
switch# show fcroute summary vsan 4
```

Send comments to nx5000-docfeedback@cisco.com

show fcs

Use the **show fcs** commands to display the status of the fabric configuration., 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 FCS.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 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. Maximum length is 255 characters.
port	Displays port objects information.
pwwn *wwn*	(Optional) 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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FCS database information:

```
switch# show fcs database
```

The following example displays interconnect element object information for a specific VSAN:

```
switch# show fcs ie vsan  1
```

This command displays interconnect element object information for a specific WWN:

```
switch# show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1
```

This command displays platform information:

```
switch# show fcs platform name SamplePlatform vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

This command displays platform information within a specified VSAN:

```
switch# show fcs platform vsan 1
```

This command displays FCS port information within a specified VSAN:

```
switch# show fcs port vsan 24
```

This command displays ports within a specified WWN:

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
```

This command displays FCS statistics:

```
switch# show fcs statistics
```

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** *vig-num/vint-id*} [statistics | wwn]]

Syntax Description

asciiwwn *ascii-wwn*	(Optional) Displays the ASCII representation of the WWN used with 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 *vig-num/vint-id*	(Optional) Specifies a virtual Fibre Channel interface (VIG number and virtual interface ID).
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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays DHCHAP configurations in FC interfaces:

```
switch# show fcsp interface fc2/3
```

The following example displays DHCHAP statistics for a FC interfaces:

```
switch# show fcsp interface fc2/3 statistics
```

The following example displays the FC-SP WWN of the device connected through a specified interface:

```
switch# show fcsp interface fc 2/1 wwn
```

The following example displays hash algorithm and DHCHAP groups configured for the local switch:

```
switch# show fcsp dhchap
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays the DHCHAP local password database:

```
switch# show fcsp dhchap database
```

The following example displays he 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 view 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 VSAN. The range is 1 to 4093.
e_d_tov	(Optional) Displays the error detection time out value (E_D_TOV) in milliseconds.
f_s_tov	(Optional) Displays the fabric stability time out 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 CFS commit or discard operation.
pending	(Optional) Displays the status of pending fctimer commands.
pending-diff	(Optional) Displays the difference between pending database and running config.
session status	(Optional) Displays the state of fctimer CFS session.
status	(Optional) Displays the Fibre Channel timer status.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured global TOVs:

```
switch# show fctimer
```

The following example displays 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	(Optional) Displays detailed information for the specified HBA entry.
hba-id	(Optional) Displays detailed information for the specified HBA entry.
vsan *vsan-id*	(Optional) Specifies FDMI information for the specified VSAN. The range is 1 to 4093.
suppress-updates	???

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all HBA management servers:

```
switch# show fdmi database
```

The following example displays VSAN1-specific FDMI information:

```
switch# show fdmi database detail vsan 1
```

The following example displays details for the specified HBA entry:

```
switch# show fdmi database detail Hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

show flogi

To list all the fabric login (FLOGI) sessions through all interfaces across all VSANs, use the **show flogi** command., show flogi {auto-area-list} | database {fcid *fcid-id* | interface {**fc** *slot*/*port* | **vfc** *vig-num*/*vint-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 *vig-num/vint-id*	Specifies a virtual Fibre Channel interface (VIG number and virtual interface ID).
vsan *vsan-id*	Displays FLOGI database entries based on the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	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

The following example displays details on the FLOGI database:

```
switch# show flogi database
```

The following example displays the FLOGI interface:

```
switch# show flogi database interface fc 2/3
```

The following example displays the FLOGI VSAN:

```
switch# show flogi database vsan 1
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays 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 VSAN ID. The range is 1 to 4093.
detail	(Optional) Displays detailed FSPF information.
domain *domain-id*	(Optional) Specifies the domain of the database. The range is 0 to 255.
interface	(Optional) Specifies the FSPF interface.
fc *slot/port*	(Optional) Specifies the Fibre Channel interface to configure.
san-port-channel *port-channel*	Specifies the port channel interface. The range is 1 to 256.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you enter the command without parameters, all the entries in the database are displayed.

Examples

The following example displays FSPF interface information:

```
switch# show fspf interface vsan 1 fc2/1
```

The following example displays FSPF database information:

```
switch# show fspf database vsan 1
```

This command displays FSPF information for a specified VSAN:

```
switch# show fspf vsan 1
```

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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the present configuration status of the in-order delivery feature:

```
switch# show in-order-guarantee
```

Send comments to nx5000-docfeedback@cisco.com

show interface

You can check the status of an interface at any time by using the **show interface** command., show interface [*interface-range*] [**bbcredit** | brief | capabilities | counters [brief] | description | transceiver [calibrations | details] | trunk vsan [*vsan-id*]]

Syntax Description

interface-range	(Optional) Displays the type of interface.
bbcredit	(Optional) Displays buffer-to-buffer credit information.
brief	(Optional) Displays brief information.
capabilities	(Optional) Displays hardware port capabilities for a specified interface.
counters	(Optional) Displays the interface counter information.
description	(Optional) Displays the interface description.
transceiver	(Optional) Displays the transceiver information for a specified interface.
calibrations	(Optional) Displays transceiver calibration information for the specified interface.
details	(Optional) Displays detailed transceiver diagnostics information for the specified interface.
trunk vsan	(Optional) Displays the trunking status of all VSANs.
vsan-id	(Optional) Displays the trunking status of the specified VSANs. The range is 1 to 4093.

Command Default

Displays information for all interfaces on the switch.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You can specify a range of interfaces by entering a command with the following example format:

interface fc1/1 - 5 , fc2/5 - 7

The spaces are required before and after the dash (-) and before and after the comma (,).

Table 8-3 lists the interface types supported by the **show interface** command.

Table 8-3 Interface Types for the show interface Command

Interface Type	Description
fc *slot/port*	Displays the Fibre Channel interface in the specified slot/port.
san-port-channel *port-channel-number*	Displays the SAN port channel interface specified by the SAN port channel number. The range is 1 to 128.

Send comments to nx5000-docfeedback@cisco.com

Table 8-3 Interface Types for the show interface Command (continued)

Interface Type	Description
vfc *vig-num/vint-id*	Displays the virtual Fibre Channel interface in the specified virtual interface group (VIG) and with the specified virtual interface ID.
vsan *vsan-id*	Displays information for a VSAN. The range is 1 to 4093.

Examples

The following example shows how to display information about a Fibre Channel interface:

```
switch# show interface fc2/3
```

The following example shows how to display information about a VSAN interface:

```
switch# show interface vsan 2
```

The following example shows how to display description information for all interfaces:

```
switch# show interface description
```

The following example shows how to display brief information for a range of interfaces:

```
switch# show interface fc2/1 - 4 brief
```

The following example shows how to display information for SAN port channel 3:

```
switch# show interface san-port-channel 3
```

The following example shows how to display information for a virtual Fibre Channel interface:

```
switch# show interface vfc2/4
```

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 FLOGI database entries based on the FCID allocated. The format is 0xhhhhhh.
source-fcid	Displays loadbalancing status for the specified source FCID. The format is 0xhhhhhh.
dest-fcid	Displays loadbalancing status for the specified destination FCID. The format is 0xhhhhhh.
exchange-id	(Optional) Displays loadbalancing status for the specified exchange. The format is 0xhhhhhh.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays 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 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 npv flogi-table

To display the information about N port virtualization (NPV) FLOGI session, use the **show npv flogi-table** command. This command has no other arguments or keywords., show npv flogi-table

Syntax Description

This command has no other keywords or arguments.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The **show npv flogi-table** command is available only when the switch is in NPV mode.

Examples

The following example displays 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 other keywords or arguments.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The **show npv flogi-table** command is available only when the switch is in NPV mode.

Examples

The following example displays 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 port index-allocation

To display port index allocation information, use the **show port index-allocation** command., show port {index-allocation [startup]}

Syntax Description

index-allocation	Displays port index allocation information.
startup	(Optional) Displays port index allocation information at startup.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Note On a switch where the maximum number of port indexes is 256, any module that exceeds that limit does not power up.

Examples

The following example displays port index allocation information at start up:

```
switch# show port index-allocation startup
```

Send comments to nx5000-docfeedback@cisco.com

show port-security

To display configured port security feature information, use the **show port-security database** command., show 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 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 1 to 100.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

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 port-security** command with the **last** *number* option, only the specified number of entries that appear first are displayed.

Send comments to nx5000-docfeedback@cisco.com

Examples

The following example displays the contents of the port security database:

```
switch# show port-security database
```

The following example displays the output of the active port security database in VSAN 1:

```
switch# show port-security database vsan 1
```

The following example displays the active database:

```
switch# show port-security database active
```

The following example displays the wildcard fWWN port security in VSAN 1:

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
```

The following example displays the configured fWWN port security in VSAN 1:

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
```

The following example displays the interface port information in VSAN 2.

```
switch# show port-security database interface fc 2/1 vsan 2
```

The following example displays the port security statistics:

```
switch# show port-security statistics
```

The following example displays the status of the active database and the autolearn configuration.

```
switch# show port-security status
```

The following example displays the previous 100 violations.

```
switch# show port-security violations
```

Related Commands

Command	Description
port-security	Configures port security parameters.

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-number*} *vsan-id* | statistics [vsan *vsan-id*]}

Syntax Description

erl	
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
history	
recent	
interface fc *slot/port*	Specifies a Fibre Channel interface.
portnumber *port-number*	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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays RLIR information for VSAN 1:

```
switch# show rlir erl vsan 1
```

The following example displays 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 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 RSCN session status.
statistics	Displays RSCN statistics.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	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

The following example displays RSCN information:

```
switch# show rscn scr-table vsan 1
```

The following example displays RSCN statistics:

```
switch# show rscn statistics vsan 1
```

The following example shows the RSCN event timeout value configured on VSAN 1:

```
switch# show rscn event-tov vsan 1
```

The following example shows 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

show san-port-channel

Use the **show san-port-channel** command to view information about existing SAN port channel configurations., show san-port-channel {compatibility-parameters | consistency [detail] | database [interface san-port-channel *port-channel-number*] | 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-channel-number*	(Optional) Specifies the SAN port channel number. The range is 1 to 256.
summary	Displays SAN port channel summary.
usage	Displays SAN port channel number usage.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SAN port channel summary:

```
switch# show san-port-channel summary
```

The following example displays the SAN port channel compatibility parameters:

```
switch# show san-port-channel compatibility-parameters
```

The following example displays the SAN port channel database:

```
switch# show san-port-channel database
```

The following example displays the consistency status of the SAN port channel database:

```
switch# show san-port-channel consistency
```

The following example displays detailed information about the consistency status of the SAN port channel database:

```
switch# show san-port-channel consistency detail
```

Send comments to nx5000-docfeedback@cisco.com

The **show san-port-channel usage** command displays details of the used and unused SAN port channel numbers:

```
switch# show san-port-channel usage
```

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-range*	(Optional) Specifies the VSAN ID or VSAN range. The ID range is 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 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 SCSI target discovery status.
tape	Displays discovered tape information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show scsi-target auto-poll** command to verify automatic discovery of online SCSI targets.

Examples

The following example displays the status of a SCSI discovery:

```
switch# show scsi-target status
```

Send comments to nx5000-docfeedback@cisco.com

The following example displays a customized discovered targets:

```
switch# show scsi-target custom-list
```

The following example displays discovered disk information:

```
switch# show scsi-target disk
```

The following example displays the discovered LUNs for all operating systems:

```
switch# show scsi-target lun os all
```

The following example displays the discovered LUNs for the Solaris operating system:

```
switch# show scsi-target lun os solaris
```

The following example displays auto-polling information:

```
switch# show scsi-target auto-poll
```

The following example displays the port WWN that is assigned to each operating system (Windows, AIX, Solaris, Linux, or HPUX):

```
switch# show scsi-target pwwn
```

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 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
Release 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays topology information:

```
switch# show topology
```

Send comments to nx5000-docfeedback@cisco.com

show trunk protocol

To display 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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays trunk protocol status:

```
switch# show trunk protocol
Trunk protocol is enabled
```

Send comments to nx5000-docfeedback@cisco.com

show vig

To display configuration details for a virtual interface group, use the **show vig** command., show vig *vig-num*

Syntax Description

vig-num	Virtual interface group number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information about the specified VIG:

```
switch# show vig 1
```

Send comments to nx5000-docfeedback@cisco.com

show vsan

To display information about configured VSAN, use the **show vsan** command., show vsan [*vsan-id* [membership] |
membership [interface {fc *slot/port* | san-port-channel *port* | **vfc** *vig-num/vint-id*}] |
usage]

Syntax Description

vsan-id	(Optional) Displays information for the specified VSAN ID. The range is 1 to 4093.
membership	(Optional) Displays membership information.
interface (Optional)	(Optional) Specifies the interface type.
fc *slot/port*	(Optional) Specifies a Fibre Channel interface.
san-port-channel *portchannel-number.subinterface-number*	(Optional) Specifies a SAN port channel interface specified by the port channel number.
vfc *vig-num/vint-id*	(Optional) Specifies a virtual Fibre Channel interface (VIG number and virtual interface ID).
usage	(Optional) Displays VSAN usage in the system.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

When you enter the **show vsan membership interface** command, interface information is displayed for interfaces that are configured in this VSAN.

The interface range must be in ascending order and non-overlapping. You can specify a range using a hyphen and several interfaces using commas:

- The interface range format for an FC interface range is **fc***slot/port* - *port* **, fc***slot/port* **, fc***slot/port*

  For example, `show int fc1/1 - 3 , fc1/5 , fc2/5`
- The format for a SAN port channel is **san-port-channel** *portchannel-number*

  For example, **show int san-port-channel 5**

Examples

The following example displays configured VSAN information:

Send comments to nx5000-docfeedback@cisco.com

```
switch# show vsan 1
```

The following example displays membership information for all VSANs.

```
switch # show vsan membership
```

The following example displays membership information for a specified interface:

```
switch # show vsan membership interface fc1/1
```

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 WWN usage and alarm status.
block-id *number*	(Optional) Displays WWN usage and alarm status for a block ID. The range is 34 to 1793.
switch	Displays switch WWN.
vsan-wwn	Displays all user-configured VSAN WWNs.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the WWN of the switch:

```
switch# show wwn switch
```

The following example displays a user-configured VSAN WWN:

```
switch# show wwn vsan-wwn
```

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 *fcid-id* [lun *lun-id*] | pwwn *wwn* [lun *lun-id*]} [active] [vsan *vsan-id*] | name *string* [pending] [active] [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-range*] vsan *vsan-id*]

Syntax Description

active	Displays zones which are part of active zone set.
vsan *vsan-id*	Displays zones belonging to the specified VSAN ID. The range is 1 to 4093.
analysis	Displays analysis of the zone database.
active	Displays analysis of the active zone database.
vsan	Displays analysis of the zone database for the specified VSAN.
zoneset	Displays analysis of the zoneset.
ess	Displays ESS information.
member	Displays all zones in which the given member is part of.
name	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 zone server current status.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured zone information:

```
switch# show zone
```

The following example displays zone information for a specific VSAN:

```
switch# show zone vsan 1
```

The following example displays members of a specific zone:

Send comments to nx5000-docfeedback@cisco.com

```
switch# show zone name Zone1
```

The following example displays all zones to which a member belongs using the FCID:

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
```

The following example displays the number of control frames exchanged with other switches:

```
switch# show zone statistics
```

The following example displays the status of the configured zones:

```
switch# show zone status
```

The following 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 8-4 describes the significant fields shown in the **show zone status vsan** display.

Table 8-4 show zone status Field Descriptions

Field	Description
VSAN:	VSAN number displayed.
default-zone:	Default-zone policy either permit or deny.
Default zone:	The Default zone field 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:	Displays interop mode. 100 = default, 1 = standard, 2 and 3 = Non-Cisco vendors.
mode:	Displays zoning mode either basic or enhanced.
merge control:	Displays merge policy either allow or restrict.
Hard zoning is enabled	If hardware resources (TCAM) becomes full, hard zoning is automatically disabled.
Full Zoning Database:	Displays values of zone database.
Active Zoning Database:	Displays values of active zone database.
Status:	Displays status of last zone distribution.

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 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	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays detailed statistics and analysis of the active zoning database:

```
switch# show zone analysis active vsan 1
```

The following example displays 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 8-5 describes the fields displayed in the output of a **show zone analysis** command for the full zoning database.

Table 8-5 show zone analysis Field Descriptions for the Full Zoning Database

Field	Description
Last updated at	Displays a time stamp showing when the full zoning database was last updated.
Last Updated by	Displays the 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	Displays the total number of zone sets in the database.
Num zones	Displays the total number of zones in the database, including unassigned zones.
Num aliases	Displays the total number of aliases in the database, including unassigned FC aliases.
Num attribute groups	Displays the 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 8-5 show zone analysis Field Descriptions (continued)for the Full Zoning Database

Field	Description
Formatted database size	Displays the 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	Displays 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.

The following example displays 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*]] | [**pending** [**active vsan** *vsan-id* | **brief** [**active vsan** *vsan-id* | **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	(Optional) Displays the VSAN.
vsan-id	Specifies the ID of the VSAN. The range is 1 to 4093
brief	(Optional) Displays zone set members in a brief list.
name	(Optional) Displays members of a specified zone set.
zoneset-name	Specifies the zone set name. The maximum is 64.
pending	(Optional) Displays zone sets members that are in session.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured zone set information:

```
switch# show zoneset vsan 1
```

The following example displays configured zone set information for a specific VSAN:

```
switch# show zoneset vsan 2-3
```

Send comments to nx5000-docfeedback@cisco.com

INDEX

A

aaa accounting default command 5-2
aaa authentication login console command 5-3
aaa authentication login default command 5-5
aaa authentication login error-enable command 5-7
aaa authentication login mschap command 5-8
aaa group server radius command 5-9
action command 5-10

B

banner motd command 1-2
boot command 1-3

C

cd command 1-5
cfs distribute command 7-2
cfs ipv4 distribute command 7-3
cfs ipv4 mcast-address command 7-5
cfs ipv6 distribute command 7-7
cfs ipv6 mcast-address command 7-9
cfs region command 7-11
cfs staggered-merge command 7-13
channel-group (Ethernet configuration) command 2-2
class-map command 4-2
clear access-list counters command 5-11
clear accounting log command 5-12
clear cli history command 1-6
clear cores command 1-7
clear debug-logfile command 1-8
clear device-alias command 7-14
clear fcdomain command 7-15
clear fcflow stats command 7-16
clear fcns statistics command 7-17
clear fcsm log command 7-18
clear fcs statistics command 7-19
clear fctimer session command 7-20
clear fspf counters command 7-21
clear install failure-reason command 1-9
clear license command 1-10
clear logging nvram command 6-2
clear logging onboard command 6-3
clear logging session command 6-4
clear mac access-list counters command 2-5
clear mac-address-table dynamic command 2-8
clear mac dynamic command 2-6
clear ntp session command 2-10
clear ntp statistics command 2-11
clear port-security command 7-22
clear rlir command 7-23
clear rscn session command 7-24
clear rscn statistics command 7-25
clear spanning-tree counters command 2-12
clear spanning-tree detected-protocol command 2-13
clear user command 1-11
clear zone command 7-26
cli var name command 1-12
clock set command 1-14
clock summer-time command 1-15
clock timezone command 1-17
configure terminal command 1-18
copy command 1-19
copy running-config startup-config command 1-23

Send comments to nx5000-docfeedback@cisco.com

D

databits command 1-24
deadtime command 5-13
debug logfile command 1-25
debug logging command 1-26
delete command 1-27
deny (IPv4) command 5-15
deny (MAC) command 5-25
description (user role) command 5-28
device-alias abort command 7-27
device-alias commit command 7-28
device-alias database command 7-29
device-alias distribute command 7-30
device-alias import command 7-31
device-alias mode command 7-32
device-alias name command 7-33
device-alias rename command 7-34
dir command 1-28
discover custom-list command 7-35
discover scsi-target command 7-36

E

echo command 1-30
end command 1-31
exec-timeout command 1-32
exit (EXEC) command 1-34
exit (global) command 1-35

F

fabric-binding activate command 7-39
fabric-binding database command 7-40
fabric-binding database diff command 7-41
fabric-binding database vsan command 7-42
fabric-binding enable command 7-44
fabric profile command 7-38
fcalias clone command 7-45
fcalias name command 7-46
fcalias rename command 7-47
fcdomain abort vsan command 7-50
fcdomain command 7-48
fcdomain commit vsan command 7-51
fcdomain distribute command 7-52
fcdomain rfc-reject command 7-53
fcdroplatency command 7-54
fcflow stats command 7-55
fcid-allocation command 7-57
fcinterop fcid-allocation command 7-58
fcns no-auto-poll command 7-59
fcns proxy-port command 7-60
fcns reject-duplicate-pwwn command 7-61
fcping command 7-62
fcroute command 7-64
fcsp command 7-69
fcsp dhchap command 7-71
fcsp enable command 7-73
fcs plat-check-global command 7-66
fcsp reauthenticate command 7-74
fcsp timeout command 7-75
fcs register command 7-67
fcs virtual-device-add command 7-68
fctimer abort command 7-77
fctimer command 7-76
fctimer commit command 7-78
fctimer distribute command 7-79
fctrace command 7-80
fdmi suppress-updates command 7-81
feature (user role feature group) command 5-29
feature fcoe command 7-82
feature interface-vlan command 2-14
feature lacp command 2-15
feature lldp command 1-36
feature private-vlan command 2-16
feature tacacs+ command 5-30
find command 1-37
format command 1-38

Send comments to nx5000-docfeedback@cisco.com

fspf config command 7-83
fspf cost command 7-85
fspf dead-interval command 7-86
fspf enable command 7-87
fspf hello-interval command 7-88
fspf passive command 7-89
fspf retransmit-interval command 7-90

G

gunzip command 1-39
gzip command 1-40

H

hostname command 1-41

I

in-order-guarantee command 7-91
install all command 1-42
install license command 1-45
instance vlan command 2-17
interface ethernet command 2-19
interface fc command 7-92
interface policy deny command 5-31
interface port-channel command 2-20
interface san-port-channel command 7-94
interface vethernet command 2-22
interface vfc command 7-97
interface vig command 7-96
ip access-list command 5-32
ip igmp snooping (EXEC) command 2-23
ip igmp snooping (VLAN) command 2-24
ip port access-group command 5-34

L

lacp port-priority command 2-26
lacp system-priority command 2-27
line console command 1-46
line vty command 1-47
lldp (interface) command 7-101
lldp command 7-99
logging abort command 7-102
logging commit command 7-103
logging console command 6-5
logging distribute command 7-104
logging level command 6-7
logging logfile command 6-9
logging module command 6-11
logging monitor command 6-13
logging server command 6-15
logging timestamp command 6-17

M

mac access-list command 5-36
mac-address-table aging-time command 2-28
mac-address-table notification command 2-30
mac-address-table static command 2-31
mac port access-group command 5-38
match command 5-40
match cos command 4-3
member (fcalias configuration submode) command 7-105
member (zone configuration submode) command 7-107
member (zoneset configuration submode) command 7-109
modem in command 1-48
modem init-string command 1-49
modem set-string user-input command 1-51
monitor session command 2-33
move command 1-52

Send comments to nx5000-docfeedback@cisco.com

N

name (MST configuration) command 2-35
name (VLAN configuration) command 2-34
npiv enable command 7-110
npv auto-load-balance disruptive command 7-111
npv enable command 7-112
ntp abort command 2-37
ntp command 2-36
ntp commit command 2-38
ntp distribute command 2-39
ntp sync-retry command 2-40

P

parity command 1-54
permit (IPv4) command 5-41
permit (MAC) command 5-51
permit interface command 5-54
permit vlan command 5-56
permit vrf command 5-58
ping command 1-55
policy-map command 4-4
port-channel load-balance ethernet command 2-41
port-security abort command 7-115
port-security command 7-113
port-security commit command 7-116
port-security database command 7-117
port-security distribute command 7-119
port-security enable command 7-120
port-track enable command 7-121
port-track force-shut command 7-122
port-track interface command 7-123
private-vlan association command 2-45
private-vlan command 2-43
private-vlan synchronize command 2-47
purge fcdomain fcid command 7-124

R

radius-server deadtime command 5-59
radius-server directed-request command 5-60
radius-server host command 5-61
radius-server key command 5-63
radius-server retransmit command 5-64
radius-server timeout command 5-65
reload command 1-57
remark command 5-66
resequence command 5-68
revision command 2-48
rlir preferred-cond fcid command 7-125
rmdir command 1-58
role feature-group name command 5-70
role name command 5-71
rscn abort command 7-128
rscn command 7-127
rscn commit command 7-129
rscn distribute command 7-130
rscn event-tov command 7-131
rule command 5-72
run-script command 1-59

S

san-port-channel persistent command 7-132
scsi-target command 7-133
send command 1-60
server command 5-74
service-policy command 4-6
session-limit command 1-62
setup command 1-61
show aaa accounting command 5-76
show aaa authentication command 5-77
show aaa groups command 5-78
show access-lists command 5-79
show accounting log command 5-80
show banner motd command 1-63

Send comments to nx5000-docfeedback@cisco.com

show boot command 1-64
show cfs command 8-2
show class-map command 4-11
show cli alias command 1-65
show cli history command 1-66
show cli variables command 1-67
show clock command 1-68
show copyright command 1-69
show debug logfile command 1-70
show debug npv command 8-4
show device-alias command 8-5
show environment command 1-71
show fabric-binding command 8-7
show fc2 command 8-9
show fcalias command 8-11
show fcdomain command 8-12
show fcdroplatency command 8-14
show fcflow stats command 8-15
show fcid-allocation command 8-16
show fcns database command 8-17
show fcns statistics command 8-19
show fcoe command 8-20
show fcroute command 8-21
show fcs command 8-23
show fcsp command 8-25
show fctimer command 8-27
show fdmi command 8-29
show file command 1-72
show flogi command 8-30
show fspf command 8-32
show hardware internal command 1-73
show hostname command 1-74
show incompatibility system command 1-75
show in-order-guarantee command 8-33
show install all command 1-76
show interface command 8-34
show interface mac-address command 3-2
show interface port-channel command 3-3
show interface priority-flow-control command 4-14
show interface private-vlan mapping command 3-4
show interface switchport command 3-5
show interface vlan command 3-6
show inventory command 1-77
show ip access-lists command 5-82
show ip igmp snooping command 3-8
show lacp command 3-9
show license command 1-78
show license host-id command 1-79
show license usage command 1-80
show line command 1-81
show lldp command 8-37
show loadbalancing command 8-36
show logging console command 6-18
show logging info command 6-19
show logging last command 6-20
show logging level command 6-21
show logging logfile command 6-22
show logging module command 6-23
show logging monitor command 6-24
show logging nvram command 6-25
show logging onboard command 6-26
show logging server command 6-31
show logging session status command 6-32
show logging status command 6-33
show logging timestamp command 6-34
show mac access-lists command 5-83
show mac-address-table aging-time command 3-10
show mac-address-table command 3-13
show mac-address-table count command 3-11
show mac-address-table notification command 3-12
show module command 1-82
show monitor session command 3-15
show npv flogi-table command 8-40
show npv status command 8-41
show policy-map command 4-10, 4-12
show policy-map interface command 4-15
show port-channel capacity command 3-16

Send comments to nx5000-docfeedback@cisco.com

show port-channel compatibility-parameters command 3-17
show port-channel database command 3-18
show port-channel load-balance command 3-19
show port-channel summary command 3-21
show port-channel traffic command 3-22
show port-channel usage command 3-23
show port index-allocation command 8-42
show port-security command 8-43
show processes command 1-83
show processes cpu command 1-84
show processes log command 1-85
show processes memory command 1-86
show radius-server command 5-84
show rlir command 8-45
show role command 5-86
show role feature command 5-87
show role feature-group command 5-88
show rscn command 8-46
show running-config aaa command 5-89
show running-config command 1-87, 3-24
show running-config diff command 1-88
show running-config radius command 5-90
show running-config security command 5-91
show running-config spanning-tree command 3-25
show running-config vlan command 3-26
show san-port-channel command 8-47
show scsi-target command 8-49
show spanning-tree active command 3-30
show spanning-tree bridge command 3-32
show spanning-tree brief command 3-34
show spanning-tree command 3-27
show spanning-tree detail command 3-36
show spanning-tree interface command 3-38
show spanning-tree mst command 3-40
show spanning-tree root command 3-42
show spanning-tree summary command 3-44
show spanning-tree vlan command 3-46
show sprom command 1-90
show ssh key command 5-92
show ssh server command 5-93
show startup-config aaa command 5-94
show startup-config command 1-91, 3-49
show startup-config radius command 5-95
show startup-config security command 5-96
show switchname command 1-92
show system cores command 1-93
show system qos command 4-13
show system reset-reason command 1-94
show system uptime command 1-95
show tacacs-server command 5-97
show tech-support command 1-96
show telnet server command 5-99
show terminal command 1-97
show topology command 8-51
show trunk protocol command 8-52
show user-account command 5-100
show users command 5-101
show version command 1-98
show vig command 8-53
show vlan access-list command 5-102
show vlan access-map command 5-103
show vlan command 3-50
show vlan filter command 5-104
show vlan id command 3-52
show vlan private-vlan command 3-53
show vsan command 8-54
show wwn command 8-56
show zone analysis command 8-59
show zone command 8-57
show zoneset command 8-62
shutdown (VLAN configuration) command 2-49
sleep command 1-99
spanning-tree bpdufilter command 2-51
spanning-tree bpduguard command 2-53
spanning-tree cost command 2-55
spanning-tree guard command 2-57
spanning-tree link-type command 2-58

Send comments to nx5000-docfeedback@cisco.com

spanning-tree loopguard default command 2-59
spanning-tree mode command 2-60
spanning-tree mst configuration command 2-61
spanning-tree mst cost command 2-63
spanning-tree mst forward-time command 2-65
spanning-tree mst hello-time command 2-66
spanning-tree mst max-age command 2-67
spanning-tree mst max-hops command 2-68
spanning-tree mst port-priority command 2-69
spanning-tree mst priority command 2-70
spanning-tree mst root command 2-71
spanning-tree mst simulate pvst command 2-73
spanning-tree mst simulate pvst global command 2-75
spanning-tree pathcost method command 2-77
spanning-tree port-priority command 2-90
spanning-tree port type edge bpdufilter default command 2-80
spanning-tree port type edge bpduguard default command 2-82
spanning-tree port type edge command 2-78
spanning-tree port type edge default command 2-84
spanning-tree port type network command 2-86
spanning-tree port type network default command 2-88
spanning-tree vlan command 2-91
speed command 1-100
ssh command 5-105
ssh key command 5-106
ssh server enable command 5-108
state command 2-93
stopbits command 1-101
storm-control level command 5-109
svi enable command 2-94
switchname command 1-104
switchport access vlan command 2-95
switchport block command 2-96
switchport command 7-135
switchport ignore bit-errors command 7-138
switchport mode private-vlan host command 2-97
switchport mode private-vlan promiscuous command 2-98
switchport private-vlan host-association command 2-99
switchport private-vlan mapping command 2-101
system cores command 1-102
system default switchport command 7-140
system default zone default-zone permit command 7-142
system default zone distribute full command 7-143
system jumbomtu command 4-8
system qos command 4-9
system startup-config unlock command 1-103

T

tacacs-server deadtime command 5-111
tacacs-server directed-request command 5-112
tacacs-server host command 5-113
tacacs-server key command 5-115
tacacs-server timeout command 5-116
tail command 1-105
telnet command 5-117
telnet server enable command 5-118
terminal length command 1-107
terminal session-timeout command 1-108
terminal terminal-type command 1-109
terminal width command 1-110
traceroute command 1-111
trunk protocol enable command 7-144

U

update license command 1-112
username command 5-121
use-vrf command 5-119

V

vlan (EXEC mode) command 2-103
vlan access-map command 5-123
vlan filter command 5-124

Send comments to nx5000-docfeedback@cisco.com

vlan policy deny command 5-126
vrf context command 2-105
vrf policy deny command 5-127
vsan database command 7-145

W

write erase command 1-113
wwn secondary-mac command 7-148
wwn vsan command 7-149

Z

zone clone command 7-150
zone commit command 7-151
zone compact command 7-152
zone copy command 7-153
zone default-zone command 7-155
zone merge-control restrict vsan command 7-156
zone mode enhanced command 7-157
zone name (configuration mode) command 7-158
zone name (zone set configuration mode) command 7-160
zone rename command 7-161
zoneset (configuration mode) command 7-162
zoneset (EXEC mode) command 7-164