Send feedback to nexus4K-docfeedback@cisco.com



Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference

Release 4.1(2)E1(1)

October 2009

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-19954-01

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0908R)

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

Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference
© 2009 Cisco Systems, Inc. All rights reserved.



Send feedback to nexus4K-docfeedback@cisco.com

CONTENTS

Preface xvii

Audience xvii

Organization xvii

Document Conventions xviii

Related Documentation xix

Obtaining Documentation and Submitting a Service Request xix

CHAPTER 1 **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 alias name 1-12

cli var name 1-14

clock set 1-16

clock summer-time 1-17

clock timezone 1-19

configure session 1-20

configure terminal 1-21

copy 1-22

copy running-config startup-config 1-26

databits 1-27

debug logfile 1-28

debug logging 1-29

delete 1-30

dir 1-32

echo 1-34

Send feedback to nexus4K-docfeedback@cisco.com

end 1-35
exec-timeout 1-36
exit (EXEC) 1-38
exit (global) 1-39
feature fip-snooping 1-40
feature interface-vlan 1-41
feature lacp 1-42
feature lst 1-43
feature private-vlan 1-44
feature ssh 1-45
feature tacacs+ 1-46
feature telnet 1-47
feature udld 1-48
find 1-49
flowcontrol hardware 1-50
format 1-51
gunzip 1-52
gzip 1-53
hostname 1-54
install all 1-55
install module bios 1-57
install license 1-58
install module epld 1-59
line com1 1-60
line console 1-61
line vty 1-62
modem connect line 1-63
modem in 1-64
modem init-string 1-65
modem restart line 1-67
modem set-string user-input 1-68
move 1-69
parity 1-71
ping 1-72
platform chassis-management protected-mode 1-73

Send feedback to nexus4K-docfeedback@cisco.com

pwd 1-75
reload 1-76
rmdir 1-77
run-script 1-78
save 1-79
send 1-80
setup 1-81
session-limit 1-82
show banner motd 1-83
show boot 1-84
show chassis summary 1-85
show cli alias 1-86
show cli history 1-87
show cli variables 1-88
show clock 1-89
show configuration session 1-90
show copyright 1-92
show debug logfile 1-93
show environment 1-94
show file 1-96
show hostname 1-97
show incompatibility system 1-98
show install all 1-99
show inventory 1-100
show license 1-101
show license host-id 1-102
show license usage 1-103
show line 1-105
show module 1-107
show processes 1-108
show processes cpu 1-109
show processes log 1-110
show processes memory 1-111
show running-config 1-112
show running-config diff 1-113

Send feedback to nexus4K-docfeedback@cisco.com

show sprom 1-115
show startup-config 1-118
show switchname 1-120
show system cores 1-121
show system internal sysmgr startup-config locks 1-122
show system reset-reason 1-123
show system uptime 1-124
show tacacs+ 1-125
show tech-support 1-126
show terminal 1-128
show version 1-129
sleep 1-131
speed 1-132
stopbits 1-133
switchname 1-134
system cores 1-135
system startup-config unlock 1-136
tail 1-137
terminal length 1-138
terminal session-timeout 1-139
terminal terminal-type 1-140
terminal width 1-141
traceroute 1-142
update license 1-143
write erase 1-144

CHAPTER 2 **Ethernet Commands** 2-1

bandwidth (interface) 2-2
cdp 2-4
cdp enable 2-6
channel-group (Ethernet) 2-7
cin 2-10
clear cdp counters 2-11
clear cdp table 2-12
clear mac access-list counters 2-13
clear mac-address-table dynamic 2-14

Send feedback to nexus4K-docfeedback@cisco.com

clear spanning-tree counters 2-16
clear spanning-tree detected-protocols 2-17
delay (interface) 2-18
description (interface) 2-19
instance vlan 2-20
interface ethernet 2-22
interface port-channel 2-23
interface vlan 2-25
ip igmp snooping (EXEC) 2-26
ip igmp snooping (VLAN) 2-27
lacp port-priority 2-29
lacp system-priority 2-30
link debounce 2-31
link state group 2-32
link state track 2-34
mac-address-table aging-time 2-35
mac-address-table notification 2-37
mac-address-table static 2-38
monitor session 2-40
name (vlan configuration) 2-41
name (mst configuration) 2-42
port-channel load-balance ethernet 2-43
private-vlan 2-45
private-vlan association 2-47
private-vlan synchronize 2-49
revision 2-50
shutdown (Vlan configuration) 2-51
spanning-tree bpdufilter 2-53
spanning-tree bpduguard 2-54
spanning-tree cost 2-56
spanning-tree guard 2-58
spanning-tree link-type 2-59
spanning-tree loopguard default 2-60
spanning-tree mode 2-61
spanning-tree mst configuration 2-62

Send feedback to nexus4K-docfeedback@cisco.com

spanning-tree mst cost 2-64
spanning-tree mst forward-time 2-66
spanning-tree mst hello-time 2-67
spanning-tree mst max-age 2-68
spanning-tree mst max-hops 2-69
spanning-tree mst port-priority 2-70
spanning-tree mst priority 2-71
spanning-tree mst root 2-72
spanning-tree mst simulate pvst 2-74
spanning-tree mst simulate pvst global 2-76
spanning-tree pathcost method 2-78
spanning-tree port type edge 2-79
spanning-tree port type edge bpdufilter default 2-81
spanning-tree port type edge bpduguard default 2-83
spanning-tree port type edge default 2-85
spanning-tree port type network 2-87
spanning-tree port type network default 2-89
spanning-tree port-priority 2-91
spanning-tree vlan 2-92
speed (Ethernet) 2-94
state 2-95
switchport access vlan 2-96
switchport block 2-97
switchport mode private-vlan host 2-98
switchport mode private-vlan promiscuous 2-99
switchport private-vlan host-association 2-100
switchport private-vlan mapping 2-102
udld (configuration mode) 2-104
udld (Ethernet) 2-106
vlan (EXEC mode) 2-108

CHAPTER 3 **Ethernet show Commands** 3-1

show cdp 3-2
show interface 3-5
show interface ethernet 3-6
show interface mac-address 3-8

Send feedback to nexus4K-docfeedback@cisco.com

show interface port-channel 3-9
show interface priority-flow-control 3-11
show interface private-vlan mapping 3-13
show interface switchport 3-14
show ip igmp snooping 3-16
show lacp 3-17
show link state group 3-18
show mac-address-table aging-time 3-20
show mac-address-table count 3-21
show mac-address-table notification 3-22
show mac-address-table 3-23
show monitor session 3-25
show port-channel load-balance 3-26
show port-channel summary 3-27
show running-config 3-28
show running-config spanning-tree 3-29
show running-config vlan 3-30
show solm cin 3-31
show solm counters 3-32
show spanning-tree 3-34
show spanning-tree active 3-37
show spanning-tree bridge 3-38
show spanning-tree brief 3-40
show spanning-tree detail 3-41
show spanning-tree interface 3-42
show spanning-tree mst 3-44
show spanning-tree mst configuration 3-46
show spanning-tree mst detail 3-47
show spanning-tree mst interface 3-48
show spanning-tree root 3-49
show spanning-tree summary 3-50
show spanning-tree vlan 3-51
show spanning-tree vlan active 3-52
show spanning-tree vlan bridge 3-53
show spanning-tree vlan brief 3-55

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan detail 3-57
show spanning-tree vlan interface 3-58
show spanning-tree vlan root 3-60
show spanning-tree vlan summary 3-62
show udld 3-63
show vlan 3-64
show vlan id 3-66
show vlan private-vlan 3-67

CHAPTER 4 **Quality of service Commands** 4-1

bandwidth (QoS) 4-2
bandwidth remaining 4-4
class 4-5
class type network-qos 4-7
class type queuing 4-8
class-map type network-qos 4-9
class-map type qos 4-10
class-map type queuing match-any 4-12
clear qos statistics 4-13
clear statistics device all 4-14
congestion-control 4-15
description 4-16
match access-group 4-17
match class-map 4-18
match cos 4-19
mtu 4-21
pause no-drop 4-22
policy-map type network-qos 4-23
policy-map type qos 4-24
policy-map type queuing 4-25
priority (queuing) 4-26
qos statistics 4-28
service-policy (interface) 4-29
set cos (policy map type qos) 4-31
shape 4-32
show class-map type network-qos 4-34

Send feedback to nexus4K-docfeedback@cisco.com

show class-map type qos 4-36
show class-map type queuing 4-37
show policy-map 4-39
show policy-map interface 4-41
show policy-map interface brief 4-43
show queuing interface 4-45
show running-config ipqos 4-47
system jumbomtu 4-49
system qos 4-50

CHAPTER 5 **Security Commands** 5-1

aaa accounting default 5-2
aaa authentication login console 5-4
aaa authentication login default 5-6
aaa authentication login error-enable 5-8
aaa authentication login mschap enable 5-9
aaa group server radius 5-10
aaa group server tacacs+ 5-11
action 5-12
clear access-list counters 5-13
clear accounting log 5-14
deadtime 5-15
deny (IPv4) 5-17
deny (MAC) 5-27
description (user role) 5-30
feature (role feature-group) 5-31
interface policy deny 5-32
ip access-list 5-33
ip port access-group 5-35
mac access-list 5-37
mac port access-group 5-39
match 5-41
object-group ip address 5-42
object-group ip port 5-43
permit (IPv4) 5-44
permit (MAC) 5-49

Send feedback to nexus4K-docfeedback@cisco.com

permit interface 5-52
permit vlan 5-54
permit vrf 5-56
radius-server deadtime 5-58
radius-server directed-request 5-59
radius-server host 5-60
radius-server key 5-63
radius-server retransmit 5-65
radius-server timeout 5-66
remark 5-67
resequence 5-69
role feature-group name 5-71
role name 5-72
rule 5-74
server 5-76
show aaa accounting 5-78
show aaa authentication 5-79
show aaa groups 5-81
show access-lists 5-82
show accounting log 5-83
show interface counters storm-control 5-85
show ip access-lists 5-87
show mac access-lists 5-88
show radius-server 5-89
show role 5-92
show role feature 5-94
show role feature-group 5-97
show running-config aaa 5-98
show running-config radius 5-100
show running-config security 5-102
show running-config tacacs+ 5-104
show ssh key 5-106
show ssh server 5-108
show startup-config aaa 5-109
show startup-config radius 5-110

Send feedback to nexus4K-docfeedback@cisco.com

show startup-config security 5-111
show startup-config tacacs+ 5-112
show tacacs-server 5-113
show telnet server 5-116
show user-account 5-117
show users 5-119
show vlan access-list 5-120
show vlan access-map 5-121
show vlan filter 5-122
ssh 5-123
ssh key 5-124
ssh server enable 5-126
statistics per-entry 5-127
storm-control 5-128
tacacs-server deadtime 5-130
tacacs-server directed-request 5-131
tacacs-server host 5-132
tacacs-server key 5-134
tacacs-server timeout 5-135
telnet 5-136
telnet server enable 5-137
use-vrf 5-138
username 5-140
vlan access-map 5-142
vlan filter 5-143
vlan policy deny 5-145
vrf policy deny 5-146

CHAPTER 6 FCoE Initialization Protocol Snooping Commands 6-1

fip-snooping enable 6-2
fip-snooping fc-map 6-3
fip-snooping port-mode fcf 6-4
interface 6-5
lldp 6-6
priority-flow-control mode 6-7
service-policy (system) 6-8

Send feedback to nexus4K-docfeedback@cisco.com

show fip-snooping enode 6-10
show fip-snooping fcf 6-11
show fip-snooping sessions 6-12
show lldp 6-13
show policy-map type network-qos 6-15
show policy-map type queuing 6-17
switchport mode trunk 6-18
switchport trunk allowed vlan 6-19

CHAPTER 7 System Management Commands 7-1
clear logging nvram 7-2
clear logging onboard 7-3
clear ntp statistics 7-4
logging console 7-5
logging event 7-7
logging event port 7-8
logging level 7-9
logging logfile 7-10
logging module 7-11
logging monitor 7-12
logging server 7-13
logging timestamp 7-14
ntp 7-15
ntp sync-retry 7-16
show logging console 7-17
show logging info 7-18
show logging last 7-20
show logging level 7-21
show logging logfile 7-22
show logging module 7-24
show logging monitor 7-25
show logging nvram 7-26
show logging onboard 7-27
show logging server 7-31
show logging timestamp 7-32
show ntp peers 7-33

Send feedback to nexus4K-docfeedback@cisco.com

show ntp statistics 7-34
show vrf 7-36
System Message Logging Facilities 7-37
vrf context 7-39

INDEX

Send feedback to nexus4K-docfeedback@cisco.com



Send feedback to nexus4K-docfeedback@cisco.com

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*, hereafter referred to as *the switch*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

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

Audience

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

Organization

This guide is organized as follows:

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

Send feedback to nexus4K-docfeedback@cisco.com

Chapter	Title	Description
Chapter 6	FCoE Initialization Protocol Snooping Commands	Describes the Cisco NX-OS FCoE Protocol Snooping commands.
Chapter 7	System Management Commands	Describes the Cisco NX-OS system management commands.

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

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

This document uses the following conventions:

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

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

Send feedback to nexus4K-docfeedback@cisco.com

Related Documentation

Documentation for Cisco Nexus 4001I Switch Module and Cisco Nexus 4005I Switch Module for IBM BladeCenter is available at the following URL:

http://www.cisco.com/go/techdocs

The following are related documents for the Cisco Nexus 4001I Switch Module and Cisco Nexus 4005I Switch Module for IBM BladeCenter:

- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter*
- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter Getting Started Guide*
- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide*
- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Release Notes*
- *Cisco NX-OS System Messages Reference*

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Send feedback to nexus4K-docfeedback@cisco.com



Send feedback to nexus4K-docfeedback@cisco.com

CHAPTER 1

Basic System Commands

This chapter describes the basic Cisco NX-OS system commands available on the switch. These commands enable you to navigate and control the switch.

Send feedback to nexus4K-docfeedback@cisco.com

banner motd

To configure the message-of-the-day (MOTD) banner that displays when the user logs in to the 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 do 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 4000 Switch" is the default MOTD string.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

boot

To configure the boot variable for the switch 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

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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:n3000.bin
```

This example shows how to configure the kickstart boot variable:

```
switch(config)# boot kickstart bootflash:n3000-kickstart.bin
```

This example shows how to clear the system boot variable:

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

Send feedback to nexus4K-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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear the debug log file:

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

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

Related Commands

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

Send feedback to nexus4K-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 No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples This example shows how to clear a specific license:

```
switch# clear license fip.lic
```

Related Commands	Command	Description
	show license	Displays license information.

Send feedback to nexus4K-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 No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

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

```
switch# clear user admin
```

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

Send feedback to nexus4K-docfeedback@cisco.com

cli alias name

To configure a command alias, use the **cli alias name** command. To remove a command alias, use the **no** form of this command.

cli alias name *alias-name alias-text*

no cli alias name *alias-name alias-text*

Syntax Description

alias-name	Name assigned to the command alias. The alias name is an alphanumeric string that is not case sensitive and must begin with an alphabetic character. The maximum length is 30 characters.
alias-text	Alias text string. The command is alphanumeric, not case sensitive, can contain spaces and special characters, and has a maximum of 100 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can use the command to create aliases for commands that you use frequently.

The Cisco NX-OS software has one predefined command alias called alias. You can use it to display the currently configured command aliases. You cannot change or remove the predefined command alias, alias.

This command does not require a license.

Examples

This example shows how to define a CLI alias name to display the system-defined type queuing class maps:

```
switch(config)# cli alias name cq show class-map type queuing
```

This example shows how to reference a CLI alias:

```
switch(config)# cq
```

This example shows how to remove a CLI alias:

```
switch(config)# no cli alias name cq
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show cli alias	Displays the CLI aliases.

Send feedback to nexus4K-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*

cli no var name *variable-name*

Syntax Description

name	Specifies a variable name.
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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

clock set

To manually set the clock on the 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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

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

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

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

configure session

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

configure session *name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to create a configuration session:

```
switch# configure session MySession
Config Session started, Session ID is 1
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-s)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

configure terminal

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

configure terminal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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).

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 feedback to nexus4K-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 are 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 feedback to nexus4K-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.
nvram:	Local NVRAM. You can copy the startup configuration to or from the nvram file system. The nvram file system is optional when referencing the startup-config file in a command.
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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 hostname.

This section contains usage guidelines for the following topics:

- Copying Files from a Server to Bootflash Memory, page 1-24
- Copying a Configuration File from a Server to the Running Configuration, page 1-24
- Copying a Configuration File from a Server to the Startup Configuration, page 1-24
- Copying the Running or Startup Configuration on a Server, page 1-24

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 feedback to nexus4K-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://192.168.2.10/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 feedback to nexus4K-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 arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

```
switch# debug logging
```

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

```
switch# no debug logging
```

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

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

Examples

This example shows how to delete a file:

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

This example shows how to delete a directory:

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

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

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

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 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 feedback to nexus4K-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
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

exit (EXEC)

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

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

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 feedback to nexus4K-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

No default behavior or values.

Command Modes

All configuration

Command History

Release	Modification
4.1(2)E1(1)	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 exits the EXEC mode and disconnects 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 feedback to nexus4K-docfeedback@cisco.com

feature fip-snooping

To enable the Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP)-snooping feature on a switch, use the **feature fip-snooping** command. To disable the FIP-snooping feature, use the **no** form of this command.

feature fip-snooping

no feature fip-snooping

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When the FIP-snooping feature is enabled, FIP packets are snooped only on the configured VLAN. Additional CE traffic is not be allowed on that VLAN after the FIP sessions are established.

This command requires a license.

Examples

This example shows how to enable the FIP-snooping feature on a switch:

```
switch(config)# feature fip-snooping
switch(config)#
```

This example shows how to disable the FIP-snooping feature on a switch:

```
switch(config)# no feature fip-snooping
switch(config)#
```

Related Commands

Command	Description
debug fip-snooping	Debugs a FIP-snooping-enabled module.
fip-snooping enable	Enables FIP snooping on a VLAN.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
interface vlan	Creates a VLAN interface.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
show lacp	Displays information on LACP.

Send feedback to nexus4K-docfeedback@cisco.com

feature lst

To enable link-state tracking (LST), which binds the link state of multiple interfaces, use the **feature lst** command. To disable LST on the switch, use the **no** form of this command.

feature lst

no feature lst

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable LST on the switch before you can configure LST groups.

Examples

This example shows how to enable LST on the switch:

```
switch(config)# feature lst
```

Related Commands

Command	Description
show link state group	Displays information about the link-state groups.

Send feedback to nexus4K-docfeedback@cisco.com

feature private-vlan

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

feature private-vlan

no feature private-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

Private VLANs are disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

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

Note A PVLAN isolated port on the 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 feedback to nexus4K-docfeedback@cisco.com

feature ssh

To enable Secure Shell (SSH) communication on the switch, use the **feature ssh** command. To disable SSH, use the **no** form of this command.

feature ssh

no feature ssh

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature ssh** command before you configure SSH features. The commands for configuring SSH are not visible until you enable SSH on the switch.

Examples

This example shows how to enable SSH:

```
switch(config)# feature ssh
```

This example shows how to disable SSH:

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

Related Commands

Command	Description
ssh	Create a SSH session using IPv4.
ssh server	Enables the SSH server.

Send feedback to nexus4K-docfeedback@cisco.com

feature tacacs+

To enable Terminal Access Controller Access Control System Plus (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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+. The commands for configuring TACACS+ server groups are not visible until you enable TACACS+.

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 feedback to nexus4K-docfeedback@cisco.com

feature telnet

To enable Telnet on the switch, use the **feature telnet** command. To disable Telnet, use the **no** form of this command.

feature telnet

no feature telnet

Syntax Description

This command has nor arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When you enable Telnet on the switch, you can create a Telnet session on the switch.

Examples

This example shows how to enable Telnet:

```
switch(config)# feature telnet
```

This example shows how to disable Telnet:

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

Related Commands

Command	Description
telnet	Creates a Telnet session using IPv4.
telnet server enable	Enables a Telnet server.

Send feedback to nexus4K-docfeedback@cisco.com

feature udld

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

feature udld

no feature udld

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable UDLD on the switch:

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

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History	Release	Modification
	4.1(2)E1(1)	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 “n3000”:

```
switch# find n3000
```

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

Send feedback to nexus4K-docfeedback@cisco.com

flowcontrol hardware

To enable flow control on the COM1 port, use the **flowcontrol hardware** command. To disable flow control, use the **no** form of this command.

flowcontrol hardware

no flowcontrol hardware

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Com1 port configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure the COM1 ports only from a session on the COM1 port.

Examples

This example shows how to enable flow control for the COM1 port:

```
switch# configure terminal
switch(config)# line com1
switch(config-com1)# flowcontrol hardware
```

This example shows how to disable flow control for the COM1 port:

```
switch# configure terminal
switch(config)# line com1
switch(config-com1)# no flowcontrol hardware
```

Related Commands

Command	Description
show line	Displays information about the COM1 port and console port configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to format the bootflash device:

```
switch# format bootflash:
```

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 the 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 feedback to nexus4K-docfeedback@cisco.com

install all

To install the kickstart and system images on the 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**.
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*
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*

Send feedback to nexus4K-docfeedback@cisco.com

Command Default

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

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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.

When you use the **install all** command with no parameters, it normalizes the system with the current running kickstart and system and upgrades any components to the version of those kickstart and system images, sets boot variables to those system and kickstart images and saves them to startup configuration.

Examples

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

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

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

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

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

```
switch# install all kickstart scp://adminuser@192.168.2.10/nx-os_kick.bin system
bootflash:scp://adminuser@192.168.2.10/nx-os_sys.bin
```

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 feedback to nexus4K-docfeedback@cisco.com

install module bios

To install a BIOS image on a switch, use the **install module bios** command.

install module *module-number* **bios** [**system** {**bootflash:** | **volatile:**} *filename*]

Syntax Description

module-number	Module number in chassis.
bootflash:	Specifies the internal Flash memory.
volatile:	Specifies the volatile memory.
filename	Name of the BIOS image file.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the BIOS image file to local storage before you can install it.

This command does not require a license.

Examples

This example shows how to install a BIOS image on the switch:

```
switch# install module 1 epld bootflash:n4000-s1-bios.4.1.2.img
```

Related Commands

Command	Description
show module	Displays information about the switch module.
show version	Displays information about the software version.

Send feedback to nexus4K-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 switches are factory installed. Manual installation is not required.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

install module epld

To install an electronically programmable logical device (EPLD) image on an I/O module, use the **install module epld** command.

install module *module-number* **epld** {**bootflash:** | **volatile:**} *filename*

Syntax Description

module-number	Module number in chassis.
bootflash:	Specifies the internal Flash memory.
volatile:	Specifies the volatile memory.
filename	Name of the EPLD image file.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the EPLD image file to local storage before you can install it.

This command does not require a license.

Examples

This example shows how to install an EPLD image on the switch:

```
switch# install module 1 epld bootflash:n4000-s1-epld.4.1.2.img
```

Related Commands

Command	Description
show module	Displays information about the switch module.
show version	Displays information about the software version.

Send feedback to nexus4K-docfeedback@cisco.com

line com1

To specify the COM1 port and enter COM1 port configuration mode, use the **line com1** command. To revert to the default configuration mode, use the **no** form of this command.

line com1

no line com1

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure the COM1 line only from a COM1 port session.

Examples

This example shows how to enter COM1 port configuration mode:

```
switch(config)# line com1
switch(config-com1)#
```

Related Commands

Command	Description
databits	Configures the number of data bits in a character for a port.
flowcontrol	Enables flow control on the COM1 port.
modem in	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 feedback to nexus4K-docfeedback@cisco.com

line console

To specify the console port and enter console port configuration mode, use the **line console** command. To revert to the default configuration mode, use the **no** form of this command.

line console

no line console

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 in	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter console port configuration mode:

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

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

modem connect line

To notify the Cisco NX-OS that you connected a modem, use the **modem connect line** command.

modem connect line {**com1** | **console**}

Syntax Description

com1	Specifies that you have connected the modem to the COM1 port.
console	Specifies that you have connected the modem to the console port.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to notify the device that you have connected a modem to the COM1 port:

```
switch# modem connect line com1
```

This example shows how to notify the device that you have connected a modem to the console port:

```
switch# modem connect line console
```

Related Commands

Command	Description
line com1	Enters COM1 port configuration mode.
line console	Enters console port configuration mode.
show line	Displays information about the COM1 and console port configuration.

Send feedback to nexus4K-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
4.1(2)E1(1)	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 com1	Enters COM1 port configuration mode.
line console	Enters console port configuration mode.
show line	Displays information about the console port configuration.

Send feedback to nexus4K-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
4.1(2)E1(1)	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
```

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

```
switch# configure terminal
```

Send feedback to nexus4K-docfeedback@cisco.com

```
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 com1	Enters COM1 port configuration mode.
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 feedback to nexus4K-docfeedback@cisco.com

modem restart line

To restart a modem connection on the COM1 port or console port, use the **modem restart line** command.

modem restart line {**com1** | **console**}

Syntax Description

com1	Restarts the modem on the COM1 port.
console	Restarts the modem on the console port.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to restart a modem connected to the COM1 port:

```
switch# modem restart line com1
```

This example shows how to restart a modem connected to the console port:

```
switch# modem restart line console
```

Related Commands

Command	Description
modem in	Enables the modem connection on the COM1 port or console port.
show line	Displays information about the COM1 and console port configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Terminal line configuration

Command History

Release	Modification
4.1(2)E1(1)	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 com1	Enters COM1 port configuration mode.
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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-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
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

ping

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

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

Syntax Description

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

Command Default

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

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

```
switch# ping 192.168.2.231
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

platform chassis-management protected-mode

To enable the protected-mode feature on the switch to prevent the Advanced Management Module (AMM) from controlling the switch, use the **platform chassis-management protected-mode** command. To disable protected mode, use the **no** form of this command.

platform chassis-management protected-mode

no platform chassis-management protected-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Note Before you enter the **platform chassis-management protected-mode** global configuration command on the switch, you must enable protected mode on the AMM.

For more information on enabling protected mode on the AMM, see the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide*.

After you enable (or disable) the protected-mode feature on the switch, you must reboot the switch so that the protected mode is operational (or nonoperational).

When protected mode is enabled, server administrators cannot manage or configure the switch from the management module. By default, this feature is disabled, and the AMM controls the switch.

After you disable the protected-mode feature on the switch, you must also disable protected mode on the AMM.

Examples

This example shows how to enable protected mode on the switch:

```
switch(config)# platform chassis-management protected-mode
switch(config)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
reload	Reloads the switch.
show chassis summary	Displays chassis information.
show running-config	Displays the running configuration.
show startup-config	Displays the startup configuration.

Send feedback to nexus4K-docfeedback@cisco.com

pwd

To view the current working directory, use the **pwd** command.

pwd

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the pwd command in configuration mode to list the name of the current working directory.

Examples

This example shows how to list the name of the current working directory:

```
switch (config)# pwd
bootflash:
switch (config)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

reload

To reload the switch, use the **reload** command.

reload {**all**}

Syntax Description		
	all	Reboot the entire switch.

Command Default Reloads the switch.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Usage Guidelines The **reload** command disrupts traffic on the switch.

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 switch:

```
switch# reload
WARNING: This command will reboot the system

Do you want to continue? (y/n) [n] y
switch#
```

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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to remove a directory:

```
switch# rmdir my_files
```

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must create the command file on a remote device and download it to the 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 feedback to nexus4K-docfeedback@cisco.com

save

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

save *location*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Session configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

Related Commands

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

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	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 feedback to nexus4K-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
4.1(2)E1(1)	This command was introduced.

Examples

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

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

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

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

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show banner motd** command and displays information about the MOTD banner:

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

Related Commands

Command	Description
banner motd	Configures the MOTD banner.

Send feedback to nexus4K-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

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples The following is sample output from the **show boot** command and displays information about all configured boot variables:

```
switch# show boot
```

The following is sample output from the **show boot variables** command and displays 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 feedback to nexus4K-docfeedback@cisco.com

show chassis summary

To display the chassis information, use the **show chassis summary** command.

show chassis summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show chassis summary** command and displays information about the chassis:

```
switch# show chassis summary
Switch Slot ID         : 10
Chassis type           : IBM BladeCenter   BC-H
Chassis ID             : KQFXBLB
Active MM in Slot      : 1

MM Stack Mode Support  : No
MM Prot Mode Support   : Yes
MM Prot Mode Status    : Operational
MM Prot Mode Config    : yes
Ext Mgmt/Ext Ports     : Disabled

Switch IP Acquisition  : static
Amm IP Acquisition     : static

VPD Def      IP  Addr  : 192.168.2.92
VPD Def      IP  Mask  : 255.255.255.0
VPD Def      Gateway   : 0.0.0.0

VPD Curr     IP  Addr  : 192.168.2.92
VPD Curr     IP  Mask  : 255.255.255.0
VPD Curr     Gateway   : 0.0.0.0
switch#
```

Related Commands

Command	Description
platform chassis-management protected-mode	Enables the protected-mode feature on the switch.

Send feedback to nexus4K-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

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples The following is sample output from the **show cli alias** command and displays information about all configured command aliases:

```
switch# show cli alias
```

The following is sample output from the **show cli alias name** command and displays information about a specific command alias:

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

Related Commands	Command	Description
	cli alias name	Configures command aliases.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show cli history** command and displays information about the command history:

```
switch# show cli history
```

The following is sample output from the **show cli history 10** command and displays the last 10 lines of the command history:

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

The following is sample output from the **show cli history unformatted** command and displays unformatted information about the command history:

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

Related Commands

Command	Description
clear cli history	Clears the command history.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show cli variables** command and displays information about the CLI variables:

```
switch# show cli variables
```

Related Commands

Command	Description
cli var name	Configures CLI variables.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show clock** command and displays the current clock setting:

```
switch# show clock
```

The following is sample output from the **show clock detail** command and displays 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 feedback to nexus4K-docfeedback@cisco.com

show configuration session

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

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

Syntax Description

session-name	(Optional) Name of an active configuration session. The session name can be maximum 64 characters.
status	(Optional) Displays the status of the active configuration sessions.
summary	(Optional) Displays a summary of the configuration session manager.

Command Default

No default behavior or values.

Command Modes

Session configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The output from the show configuration session command is very long. To better manage this output, you can redirect the output to a file (for example **show configuration session** > *filename*) in the local writable storage file system or the remote file system.

The syntax for the filename string is as follows:

filesystem://server/directory/filename

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

Use the URL prefix keywords for local writable storage file systems or remote file systems. 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.

Examples

The following is sample output from the **show configuration session** command and displays information about the current active session:

```
switch(config-s)# show configuration session
config session MySession

Number of active configuration sessions = 1
switch(config-s)#
```

The following is sample output from the **show configuration session status** command and displays the status information of the current active session:

```
switch(config-s)# show configuration session status
==============================================================================
```

Send feedback to nexus4K-docfeedback@cisco.com

```
Session Name          : MySession
Last Action           : None
Last Action Status    : Success
Last Action Reason    : -NA-
Last Action Timestamp : 00:00:00 UTC Jan 01 1970
==============================================================================

switch(config-s)#
```

The following is sample output from the **show configuration session summary** command and displays information about the current active session:

```
switch(config-s)# show configuration session summary
Session Manager Database:
------------------------------------------------------------------
Name                    Session Owner           Creation Time
------------------------------------------------------------------
MySession               root                    03:55:45 UTC Jul 13 2009

Number of active configuration sessions = 1
switch(config-s)#
```

Related Commands

Command	Description
configure session	Configures a session.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show copyright** command and displays the Cisco NX-OS copyright information:

```
switch# show copyright
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

Related Commands

Command	Description
show version	Displays information about the software version.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following is sample output from the **show debug logfile** command and displays the contents of a debug log file:

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

Related Commands.

Command	Description
debug logfile	Configures the debug log file.

Send feedback to nexus4K-docfeedback@cisco.com

show environment

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

show environment [> *filename* | >> *filename* | **temperature**]

Syntax Description

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

Command Default

Displays the status of the switch temperature.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The output of this command may be large. To better manage this output, you can redirect the output to a file (for example **show environment** > *filename*) in the local writable storage file system or the remote file system.

The syntax for the filename string is as follows:

filesystem://server/directory/filename

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

Use the URL prefix keywords for local writable storage file systems or remote file systems. 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.

Examples

The following is sample output from the **show environment** command and displays information about the hardware environment:

```
switch# show environment

Temperature
--------------------------------------------------------------------
Module   Sensor     MajorThresh   MinorThres   CurTemp     Status
                    (Celsius)     (Celsius)    (Celsius)
--------------------------------------------------------------------
1        Outlet-1   75            60           29          ok
1        Outlet-2   75            60           31          ok
1        Outlet-3   65            50           39          ok
1        Outlet-4   65            50           40          ok
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch#
```

The following is sample output from the **show environment temperature** command and displays information about the temperature environment:

```
switch# show environment temperature
```

Related Commands

Command	Description
show module	Displays module information.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show file** command and displays the contents of a file:

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

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

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

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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following is sample output from the **show hostname** command and displays the hostname assigned to the switch:

```
switch-nx4# show hostname
switch-nx4
switch-nx4#
```

Related Commands

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

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show incompatibility system** command and displays 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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show install all failure-reason** command and displays the installation failure reason:

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

The following is sample output from the **show install all impact** command and displays information about the impact of installing new images:

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

The following is sample output from the **show install all status** command and displays 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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show inventory** command and displays information about the switch hardware inventory:

```
switch# show inventory
NAME: "Chassis", DESCR: "Nexus4K Chassis"
PID: DS-C9134-K9       , VID: V01 , SN: JAB1251002X

NAME: "Module 1", DESCR: "DCE Supervisor Module-Nx4k"
PID: DS-C9134-K9-SUP   , VID: V01 , SN: JAB1251002X

switch#
```

Related Commands

Command	Description
show module	Displays information about the modules.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show license file** command and displays information about a specific license installed on the switch:

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

The following is sample output from the **show license brief** command and displays a list of license files installed on a device:

```
switch# show license brief
```

The following is sample output from the **show license** command and displays 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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following is sample output from the **show license host-id** command and displays information about the host ID required to request node-locked licenses:

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

Related Commands

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

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show license usage** command and displays information about the current license usage:

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

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

Table 1-6 show license usage Columns

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

Send feedback to nexus4K-docfeedback@cisco.com

Table 1-6 show license usage Columns (continued)

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

The following is sample output from the **show license usage** command and displays 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 feedback to nexus4K-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 terminal port configuration.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show line** command and displays information about the terminal port configuration:

```
switch# show line
line Console:
    Speed:        9600 baud
    Databits:     8 bits per byte
    Stopbits:     1 bit(s)
    Parity:       none
    Modem In: Disable
    Modem Init-String -
        default : ATE0Q1&D2&C1S0=1\015

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

switch#
```

The following is sample output from the **show line console** command and displays information about the console port configuration:

```
switch# show line console
line Console:
    Speed:        9600 baud
    Databits:     8 bits per byte
    Stopbits:     1 bit(s)
    Parity:       none
    Modem In: Disable
    Modem Init-String -
```

Send feedback to nexus4K-docfeedback@cisco.com

```
        default : ATE0Q1&D2&C1S0=1\015
switch#
```

Related Commands

Command	Description
line com1	Enters the COM1 port configuration mode.
line console	Enters the console port configuration mode.

Send feedback to nexus4K-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 1.

Command Default Displays module information for all modules in the switch chassis.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples The following is sample output from the **show module** command and displays information about all modules in the chassis:

```
switch# show module
Mod Ports  Module-Type                       Model                 Status

--- -----  -------------------------------- ---------------------- ------------
1    20     DCE Supervisor Module-Nx4K      DS-C9134-K9-SUP        active *

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

---  --------------  ------  --------------------------------------------------
1    4.1(2)E1(1)     6.0     --

Mod  MAC-Address(es)                         Serial-Num

---  --------------------------------------  ----------
1    0005.ad00.37aa to 0005.ad00.37d1         JAB1303003S
switch#
```

Related Commands	Command	Description
	show inventory	Displays hardware inventory information.

Send feedback to nexus4K-docfeedback@cisco.com

show processes

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

show processes

Syntax Description

This command has no arguments or keywords.

Command Default

Displays information for all processes running on the switch.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show processes** command and displays information about 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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show processes cpu** command and displays information about 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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show processes log** command and displays summary information about the process log:

```
switch# show processes log
```

The following is sample output from the **show processes log details** command and displays detailed information about the process log:

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

The following is sample output from the **show processes log pid** command and displays information about 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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show processes memory** command and displays information about the memory allocation for processes:

```
switch# show processes memory
```

The following is sample output from the **show processes memory shared** command and displays information about the 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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config** command and displays information about the changes that you have made to the running configuration:

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

The following is sample output from the **show running-config all** command and displays information about 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.
platform chassis-management protected-mode	Enables or disables protected mode on the chassis management module of the switch.
show running-config diff	Displays the differences between the running configuration and the startup configuration.
show startup-config	Displays the startup configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Table 1-7 show running-config diff Notations

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

Examples

The following is sample output from the **show running-config diff** command and displays information about the difference between the running configuration and the startup configuration:

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

Send feedback to nexus4K-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 feedback to nexus4K-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** [> | >> | | *type*] | **module** *module-number* | **sup** [> *filename* | >> *filename* | | *type*]}

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 an I/O module. The module number range is from 1 to 3.
sup	Displays the SPROM contents for the active supervisor module.
> *filename*	Redirects the output to a file.
>> *filename*	Redirects the output to a file in append mode.
| *type*	Filters the output based on the specified *type*.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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.

Redirecting the Output to a File

The output from the **show sprom session** command is very long. To better manage this output, you can redirect the output to a file in the local writable storage file system or the remote file system.

The syntax for the filename string is as follows:

filesystem://*server*/*directory*/*filename*

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

Use the URL prefix keywords for local writable storage file systems or remote file systems. 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. For remote file systems, if it is not otherwise specified, the path is the default for the user on the remote server.

Send feedback to nexus4K-docfeedback@cisco.com

Filtering Output

Table 1-8 lists the valid values for filter *type*:

Table 1-8 Filter Types

Filter	Description
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 the expression.
count [> *file* | | *type*]	Counts number of lines.
cut	Print selected parts 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 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 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*]	Includes 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 the expression.
last [*num*]	Displays the last lines to print. The optional *num* specifies the number of lines to print. Range: 0 to 9999.

Send feedback to nexus4K-docfeedback@cisco.com

Table 1-8 Filter Types (continued)

Filter	Description
less [-E | -d]	Quits at the end of the file. • **-E**—(Optional) Quits at the end of the file. • **-d**—(Optional) Specifies a dumb terminal.
no-more	Turns-off pagination for command output.
sed *command*	Stream Editor
sort	Sorts the output.
tr	Copies the output by substituting or deleting selected characters.
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.
uniq	Filters out repeated lines in a file.

Examples

The following is sample output from the **show sprom all** command and displays the SPROM information for all components on the physical device:

```
switch# show sprom all
```

The following is sample output from the **show sprom all | head** command and displays the first 10 lines of the SPROM information:

```
switch# show sprom all | head
DISPLAY backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x14da
 EEPROM Size     : 65535
 Block Count     : 6
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
switch#
```

The following is sample output from the **show sprom backplane** command and displays the SPROM information for the backplane:

```
switch# show sprom backplane
```

Related Commands

Command	Description
show inventory	Displays hardware inventory information.

Send feedback to nexus4K-docfeedback@cisco.com

show startup-config

To display the contents of the currently running configuration file, use the **show startup-config** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show startup-config** command and displays information about the startup configuration file:

```
switch# show startup-config
version 4.1(2)E1(1)
feature telnet
no feature ssh
feature fip-snooping

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network
-operator
username admin password 5 $1$zkTYLs/y$sOecMEkhsnJT8Lu8rbPAQ/  role network-admin
username USERID password 5 $1$8UHo5rdt$6zLdUqn4dr3Aqk0DFyBlq.  role network-oper
ator

banner motd #Nexus 4000 Switch#

ip domain-lookup
ip host nexus4k 192.168.2.168
switchname nexus4k
policy-map type queuing policy-fcoe-bandwidth
  class type queuing 1p7q4t-out-q-default
    bandwidth percent 50
class-map type network-qos class-fcoe
  match cos 3
class-map type network-qos class-non-fcoe
  match cos 0-2,4-7
policy-map type network-qos policy-fcoe
  class type network-qos class-fcoe
    pause no-drop
    mtu 2500
  class type network-qos class-non-fcoe
system qos
  service-policy type network-qos policy-fcoe
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  service-policy type queuing output policy-fcoe-bandwidth
snmp-server user admin network-admin auth md5 0x30ab109e688ce7e4d349b7a573b164b1
 priv 0x30ab109e688ce7e4d349b7a573b164b1 localizedkey
snmp-server user USERID network-operator auth md5 0xc6514896c567734524fcd3abd083
95dc priv 0xc6514896c567734524fcd3abd08395dc localizedkey

vrf context management
vlan 1

interface Ethernet1/1

interface Ethernet1/2

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface mgmt0

interface mgmt1
boot kickstart bootflash:/taishan_kickstart.4.1.2.E1.0.151.gbin
boot system bootflash:/new_n4k_image.bin
system health loopback frequency 60

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
platform chassis-management protected-mode	Enables or disables protected mode on the chassis management module of the switch.
show running-config	Displays the running-configuration.
show running-config diff	Displays the differences between the running configuration and the startup configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following is sample output from the **show switchname** command and displays information about 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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following is sample output from the **show system cores** command and displays information about the system core files:

```
switch# show system cores
```

Related Commands

Command	Description
system cores	Configures the system core filename.

Send feedback to nexus4K-docfeedback@cisco.com

show system internal sysmgr startup-config locks

To display the startup configuration locks, use the **show system internal sysmgr startup-config locks** command.

show system internal sysmgr startup-config locks

Syntax Description

internal	Commands for internal use.
sysmgr	Displays the internal state of the System Manager.
startup-config	Displays the startup-config update debugging information.
locks	Displays the startup configuration locks that are held by the system.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show system internal sysmgr startup-config locks** command and displays information about the startup configuration locks:

```
switch# show system internal sysmgr startup-config locks
```

Related Commands

Command	Description
system startup-config unlock	Unlocks the system configuration file.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show system reset** command and displays information about the reset-reason history for the switch:

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 499268 usecs after Sun Jul 12 23:30:48 2009
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 4.1(2)E1(0.130)

2) At 588818 usecs after Sun Jul 12 21:50:57 2009
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 4.1(2)E1(0.130)

3) At 808446 usecs after Sun Jul 12 20:51:43 2009
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 4.1(2)E1(0.130)
switch#
```

Related Commands

Command	Description
reload	Reloads the switch.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show system uptime** command and displays the amount of time since the last system restart:

```
switch# show system uptime
System start time:          Sun Jul 12 23:32:45 2009
System uptime:              0 days, 5 hours, 31 minutes, 55 seconds
Kernel uptime:              0 days, 5 hours, 33 minutes, 8 seconds
Active supervisor uptime:   0 days, 5 hours, 31 minutes, 55 seconds
switch#
```

Related Commands

Command	Description
reload	Reloads the switch.
show switchname	Displays the hostname for the device.

Send feedback to nexus4K-docfeedback@cisco.com

show tacacs+

To display Terminal Access Controller Access Control System Plus (TACACS+) configuration information, use the **show tacacs+** command.

show tacacs+ {**session status** | **status**}

Syntax Description

session status	Show TACACS Cisco Fabric Services (CFS) session status.
status	Show TACACS CFS distribution status.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command to enable TACACS+ before you can display TACACS configuration information.

Examples

The following is sample output from the **show tacacs+ status** command and displays the TACACS+ status information:

```
switch(config)# show tacacs+ status
distribution : disabled
session ongoing: no
session db: does not exist
merge protocol status:

last operation: none
last operation status: none
switch(config)#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show tech-support** command and displays information about the technical support:

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

This example shows how to redirect the technical support information to a file:

```
switch# show tech-support > bootflash:TechSupport.txt
```

The following is sample output from the **show tech-support brief** command and displays the brief technical support information for the switch:

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

The following is sample output from the **show tech-support** command and displays the technical support information for a specific feature:

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

The following is sample output from the **show tech-support commands** command and displays information about the commands used to generate the technical support information:

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

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show switchname	Displays the hostname for the device.
show system-uptime	Displays the amount of time since the last system restart.
show interface vlan	Displays brief descriptive information about specified VLANs.
show inventory	Displays the physical inventory information for the switch hardware, use the show inventory command.
show version	Displays information about the software version.
show logging logfile	Displays the messages in the log file that were timestamped within the span entered.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show terminal** command and displays 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 terminal-type	Configures the terminal type for a session.
terminal width	Configures the terminal display width for a session.

Send feedback to nexus4K-docfeedback@cisco.com

show version

To display information about the software version, use the **show version** command.

show version [**image** *filename* | **module** *module-number* **epld**]

Syntax Description

image *filename*	(Optional) Displays the version information for a system or kickstart image file.
module	(Optional) Displays the software version information of the module.
module-number	Module number on the chassis.
epld	Displays the current electronically programmable logical device (EPLD) versions of the module.

Command Default

Displays software version information for the running kickstart and system images.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show version** command and displays the version information for the kickstart and system image running on the device:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.0.25
  loader:    version N/A
  kickstart: version 4.1(2)E1(1) [build 4.1(2)E1(0.106)] [gdb]
  system:    version 4.1(2)E1(1) [build 4.1(2)E1(0.106)] [gdb]
  BIOS compile time:       05/08/09
  kickstart image file is: bootflash:///taishan_kickstart.4.1.2.E1.0.106.gbin
  kickstart compile time:  6/8/2009 0:00:00 [06/08/2009 11:08:39]
  system image file is:    bootflash:///taishan_system.4.1.2.E1.0.106.gbin
  system compile time:     6/8/2009 0:00:00 [06/08/2009 10:56:24]

Hardware
  cisco Nexus4K Chassis ("DCE Supervisor Module-Nx4K")
  Motorola, e500v2  with 2076512 kB of memory.
  Processor Board ID JAB1303003S
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  Device name: nexus4k35
  bootflash:     826828 kB

Kernel uptime is 0 day(s), 0 hour(s), 2 minute(s), 56 second(s)

Last reset at 29427 usecs after  Mon Jun 15 06:05:21 2009

  Reason: Reset Requested by CLI command reload
  System version: 4.1(2)E1(0.001)
  Service:

plugin
  Core Plugin, Ethernet Plugin
switch#
```

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

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

Related Commands

Command	Description
show copyright	Displays the Cisco NX-OS software copyright information.
show system reset-reason	Displays the reset history for the switch.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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
4.1(2)E1(1)	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 feedback to nexus4K-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
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 the 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 feedback to nexus4K-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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to configure a core file:

```
switch# configure terminal
switch(config)# system cores tftp://serverA:69/core_file
```

This example shows how to disable system core logging:

```
switch# configure terminal
switch(config)# no system cores
```

Related Commands

Command	Description
show system cores	Displays the core filename.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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
```

Related Commands

Command	Description
show system internal sysmgr startup-config locks	Displays the startup configuration locks being held.

Send feedback to nexus4K-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**, **debug**, 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. Valid values are 0 to 80.

Command Default

Displays the last 10 lines.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Do not include spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Examples

This example shows how to display the last 10 lines of a file:

```
switch# tail bootflash:startup.cfg
```

This example shows how to display the last 20 lines of a file:

```
switch# tail bootflash:startup.cfg 20
```

Related Commands

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

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

traceroute

To discover the routes that packets take when traveling to an IP address, use the **traceroute** command.

traceroute {*dest-addr* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}] [**source** *src-addr*]

Syntax Description

dest-addr	IP address of the destination device. The format is *A.B.C.D*.
hostname	Name of the destination device. The name is case sensitive.
vrf {*vrf-name* | **default** | **management**}	(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*. The default is the IPv4 address for the management interface of the switch.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

```
switch# traceroute 192.168.2.168 vrf management
traceroute to 192.168.2.168, 30 hops max, 40 byte packets
 1 192.168.2.168 1.922 ms  0.865 ms  0.779 ms
switch#
```

Related Commands

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

Send feedback to nexus4K-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.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

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 feedback to nexus4K-docfeedback@cisco.com

write erase

To erase the 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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com



CHAPTER 2

Ethernet Commands

This chapter describes the Cisco NX-OS Ethernet commands available on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

bandwidth (interface)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command. To restore the default values, use the **no** form of this command.

bandwidth {*kbps* | **inherit** [*kbps*]}

no bandwidth {*kbps* | **inherit** [*kbps*]}

Syntax Description

kbps	Informational bandwidth in kilobits for each second. Valid values are from 1 to 10000000.
inherit	(Optional) Specifies the bandwidth inherited from the main interface.

Command Default

1000000 kbps.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols. You cannot adjust the actual bandwidth of an interface using this command.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If a bandwidth is not configured on a subinterface, and you use the **bandwidth inherit** command, all subinterfaces inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces use this new value.

If you do not configure a bandwidth on the subinterface and you configure the bandwidth inherit command on the main interface, the subinterfaces inherit the specified bandwidth.

In all cases, if an interface has an explicit bandwidth setting configured, then that interface uses that setting, regardless of whether the bandwidth inheritance setting is in effect.

Examples

This example shows how to configure all subinterfaces off this main interface to inherit the configured bandwidth:

```
switch(config-if)# bandwidth inherit 30000
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send feedback to nexus4K-docfeedback@cisco.com

cdp

To enable the Cisco Discovery Protocol (CDP) and configure CDP attributes, use the **cdp** command. To disable CDP or reset CDP attributes, use the **no** form of this command.

cdp {**advertise** {**v1** | **v2**} | **enable** | **format device-id** {**mac-address** | **serial-number** | **system-name**} | **holdtime** *seconds* | **timer** *seconds*}

no cdp {**advertise** | **enable** | **format device-id** {**mac-address** | **serial-number** | **system-name**} | **holdtime** *seconds* | **timer** *seconds*}

Syntax Description

advertise {**v1** | **v2**}	Configures the version to use to send CDP advertisements. Version 2 is the default state.
enable	Enables CDP for all Ethernet interfaces.
format device-id	Configures the format of the CDP device ID.
mac-address	Use the MAC address as the CDP device ID.
serial-number	Use the serial number as the CDP device ID.
system-name	Use the system name, which can be expressed as a fully qualified domain name, as the CDP device ID. This is the default.
holdtime *seconds*	Specifies the amount of time a receiver should hold CDP information before discarding it. The range is from 10 to 255 seconds. The default is 180 seconds.
timer *seconds*	Sets the transmission frequency of CDP updates in seconds. The range is from 5 to 254. The default is 60 seconds.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You cannot disable CDP advertisement Version 2.

Examples

This example shows how to enable CDP on all Ethernet interfaces:

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

This example shows how to configure the MAC address as the CDP device ID:

```
switch# configure terminal
switch(config)# cdp format device-id mac-address
```

Send feedback to nexus4K-docfeedback@cisco.com

This example shows how to disable CDP on all Ethernet interfaces:

```
switch# configure terminal
switch(config)# no cdp enable
```

Related Commands

Command	Description
show cdp	Displays Cisco Discovery Protocol (CDP) information.

Send feedback to nexus4K-docfeedback@cisco.com

cdp enable

To enable the Cisco Discovery Protocol (CDP) on an Ethernet interface, use the **cdp enable** command. To disable CDP on the interface, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable CDP on an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# cdp enable
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send feedback to nexus4K-docfeedback@cisco.com

channel-group (Ethernet)

To assign and configure a physical interface to an EtherChannel, use the **channel-group** command. To remove the channel group configuration from the interface, use the **no** form of this command.

channel-group *number* [**mode** {**active** | **on** | **passive**}]

no channel-group [*number*]

Syntax Description

number	EtherChannel group number. Valid values are from 1 to 576. Cisco NX-OS creates the EtherChannel associated with this channel group if the EtherChannel does not already exist.
mode	(Optional) Specifies the EtherChannel mode of the interface.
active	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. 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 EtherChannels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the switch returns an error message. After you enable LACP globally, by using the **feature lacp** command, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface. It does not join the channel group. The default mode is **on**.
passive	Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected. The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Send feedback to nexus4K-docfeedback@cisco.com

Usage Guidelines

Use this command to create a channel group that includes the interface that you are working on and to add or remove specific interfaces from the channel group. Use this command to move a port from one channel group to another. You enter the channel group that you want the port to move to. The switch automatically removes the specified port from its present channel group and adds it to the specified channel group.

After you enable LACP globally, by using the **feature lacp** command, you enable LACP on each channel by configuring the channel mode as either **active** or **passive**. An EtherChannel in the **on** channel mode is a pure EtherChannel and can aggregate a maximum of eight ports. The EtherChannel does not run LACP.

You cannot change the mode for an existing EtherChannel or any of its interfaces if that EtherChannel is not running LACP. The channel mode remains as **on**. The system returns an error message if you attempt to change the mode.

Use the **no** form of this command to remove the physical interface from the EtherChannel. When you delete the last physical interface from an EtherChannel, the EtherChannel remains. To delete the EtherChannel completely, use the **no interface port-channel** command.

The compatibility check includes the following operational attributes:

- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- SPAN (cannot be SPAN source or destination port)
- Storm control

Use the **show port-channel compatibility-parameters** command to see the full list of compatibility checks that Cisco NX-OS uses.

You can only add interfaces configured with the channel mode set to **on** for static EtherChannels, that is, without a configured aggregation protocol. You can only add interfaces configured with the channel mode as **active** or **passive** to EtherChannels that are running LACP.

You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, Cisco NX-OS suspends that port in the EtherChannel.

When the interface joins an EtherChannel, some of its individual parameters are overridden with the values on the EtherChannel, as follows:

- MAC address
- Spanning Tree Protocol (STP)
- Service policy
- Quality of service (QoS)
- Access control lists (ACLs)

Interface parameters, such as the following, remain unaffected when the interface joins or leaves an EtherChannel:

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

Send feedback to nexus4K-docfeedback@cisco.com

- Debounce
- Rate mode
- Shutdown
- SNMP trap

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

Any configuration changes that you make in any of the compatibility parameters to the EtherChannel interface are propagated to all interfaces within the same channel group as the EtherChannel (for example, configuration changes are also propagated to the physical interfaces that are not part of the EtherChannel but are part of the channel group).

Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 mode active
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

cin

To configure a VLAN as a CIN (Chassis Internal Network) VLAN, use the **cin** command. To remove this configuration, use the **no** form of this command.

cin

no cin

Syntax Description

This command has no arguments or keywords.

Command Default

Not shut down.

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure the VLAN as a CIN VLAN only from a session on the VLAN port.

Examples

This example shows how to configure a VLAN as a CIN VLAN:

```
switch (config)#
switch (config)# vlan 5
switch (config-vlan)# cin
```

This example shows how to remove VLAN as a CIN VLAN:

```
switch (config)# vlan 5
switch (config-vlan)# no cin
```

Related Commands

Command	Description
show solm cin	Displays information about the CIN VLANs.
show solm counters	Displays the Ingress and Egress counters for CIN VLANs.

Send feedback to nexus4K-docfeedback@cisco.com

clear cdp counters

To clear the Cisco Discovery Protocol (CDP) counters, use the **clear cdp counters** command.

clear cdp counters [**interface** {**ethernet** *slot* | **mgmt** *mgmt*}]

Syntax Description

interface	(Optional) Specifies the type of interface.
ethernet	Specifies the Ethernet IEEE 802.3 interface.
slot	Ethernet interface slot number and port number specified in the format 1/1.
mgmt	Specifies the management interface.
mgmt	Management interface number. The range is from 0 to 1.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear CDP counters in a management interface:

```
switch (config)# clear cdp counters interface mgmt 0
switch (config)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

clear cdp table

To clear a Cisco Discovery Protocol (CDP) table, use the **clear cdp table** command.

clear cdp table [**interface** {**ethernet** *slot* | **mgmt** *mgmt*}]

Syntax Description

interface	Specifies the type of interface.
ethernet	Specifies the Ethernet IEEE 802.3 interface.
slot	Ethernet interface slot number and port number specified in the format 1/1.
mgmt	Specifies the management interface.
mgmt	Management interface number. The range is from 0 to 1.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear a CDP table in a management interface:

```
switch (config)# clear cdp table interface mgmt 0
switch (config)#
```

Related Commands

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

Send feedback to nexus4K-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. The name can be 64 characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear statistical information from the access list:

```
switch# clear mac access-list counters
```

Related Commands

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

Send feedback to nexus4K-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** {**ethernet** *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	(Optional) Specifies the interface for which MAC addresses should be removed from the table.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface slot and port number in the format 1/1.
port-channel *number*	(Optional) Specifies the EtherChannel for which MAC addresses should be removed from the table. Use the EtherChannel number. Valid values are 1 to 576.
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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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.

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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

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

Send feedback to nexus4K-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** *slot/port* | **port-channel** *number*} | **vlan** *vlan-id*]

Syntax Description

interface	(Optional) Specifies the interface type.
ethernet *slot/port*	Ethernet interface slot and port number. The slot and port number is specified in the format 1/1.
port-channel *number*	EtherChannel number. Valid values are 1 to 576.
vlan *vlan-id*	(Optional) Specifies the VLAN. The range is from 1 to 4094.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can clear all the STP counters on the entire switch, for each VLAN, or for each 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 feedback to nexus4K-docfeedback@cisco.com

clear spanning-tree detected-protocols

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** *slot/port* | **port-channel** *number*}]

Syntax Description

interface	(Optional) Specifies the interface type.
ethernet *slot/port*	Ethernet interface slot and port number specified in the format 1/1.
port-channel *number*	EtherChannel number. Valid values are 1 to 576.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

delay (interface)

To set a delay value for an interface, use the **delay** command. To restore the default delay value, use the **no** form of this command.

delay *tens-of-microseconds*

no delay

Syntax Description

tens-of-microseconds	Specifies the throughput delay in tens of microseconds. Valid values are 1 to 16777215 microseconds.

Command Default

10 µsec.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following example shows how to set a delay of 30,000 microseconds on an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# delay 3000
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send feedback to nexus4K-docfeedback@cisco.com

description (interface)

To add a description to an interface configuration, use the **description** command. To remove the description, use the **no** form of this command.

description *description*

no description

Syntax Description

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

Command Default

No description is added.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **description** command provides a reminder in the configuration to describe what certain interfaces are used for. The description appears in the output of the following commands such as **show interface** and **show running-config**.

Examples

The following example shows how to add a description for an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# description "10G Server Link"
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.
show running-config	Displays the contents of the currently running configuration file.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

interface ethernet

To enter interface configuration mode for an 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 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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
show interface ethernet	Displays various parameters of an Ethernet IEEE 802.3 interface.

Send feedback to nexus4K-docfeedback@cisco.com

interface port-channel

To create an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command. To remove an EtherChannel interface, use the **no** form of this command.

interface port-channel *channel-number*

no interface port-channel *channel-number*

Syntax Description

channel-number	Channel number that is assigned to this EtherChannel logical interface. The range of valid values is from 1 to 576.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

A port can belong to only one channel group.

When you use the **interface port-channel** command, follow these guidelines:

- If you are using CDP, you must configure it only on the physical interface and not on the EtherChannel interface.
- If you do not assign a static MAC address on the EtherChannel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the EtherChannel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

Examples

This example shows how to create an EtherChannel group interface with channel-group number 50:

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

Related Commands

Command	Description
switchport access vlan	Sets the access mode of the interface to a specified VLAN.
show interface port-channel	Displays information on traffic on the specified EtherChannel interface.

Send feedback to nexus4K-docfeedback@cisco.com

Command	Description
show lacp	Displays LACP information.
show port-channel summary	Displays summary information on the EtherChannels.

Send feedback to nexus4K-docfeedback@cisco.com

interface vlan

To create a VLAN interface and enter interface configuration mode, use the **interface vlan** command. To remove a VLAN interface, use the **no** form of this command.

interface vlan *interface-number*

no interface vlan *interface-number*

Syntax Description

interface-number	VLAN interface number. Valid values are 1 to 4094.

Command Default

No default behavior or values.

Command Modes

Configuration

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable interface VLANs by using the **feature interface-vlan** command. The commands for configuring interface VLANs are not visible until you enable this feature.

Examples

This example show how to create a VLAN interface:

```
switch(config)# interface vlan 3
switch(config-if)#
```

Related Commands

Command	Description
feature interface-vlan	Enables VLAN interfaces on a switch.
private-vlan	Configures private VLANs.
show vlan private-vlan	Displays private VLAN information.
shutdown	Enables or disables local traffic on a VLAN.

Send feedback to nexus4K-docfeedback@cisco.com

ip igmp snooping (EXEC)

To enable Internet Group Management Protocol (IGMP), use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP snooping is enabled.

Note If the global setting is disabled, all VLANs are treated as disabled, whether they are enabled or not.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable IGMP snooping:

```
switch(config)# ip igmp snooping
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information and configuration.

Send feedback to nexus4K-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 [explicit-tracking | fast-leave | last-member-query-interval *seconds* **| link-local-groups-suppression | mrouter interface {ethernet** *slot* **| port-channel** *number***} | querier** *IP-address* **| report-suppression | static-group** *group-IP-address***]**

no ip igmp snooping [**explicit-tracking** | **fast-leave** | **last-member-query-interval** *seconds* | **link-local-groups-suppression** | **mrouter interface** {**ethernet** *slot* | **port-channel** *number*} | **querier** *IP-address* | **report-suppression** | **static-group** *group-IP-address* [**interface** {**ethernet** *slot* | **port-channel** *number*} | **source** *source-ip-addr*]]

Syntax Description

explicit-tracking	Enables tracking IGMPv3 membership reports for each port on a VLAN and for each VLAN. 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.
link-local-groups-suppression	Configures VLAN link-local groups suppression.
mrouter interface	Configures a static connection to a multicast router. The specified interface is Ethernet or EtherChannel.
ethernet *slot*	Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
port-channel *number*	EtherChannel number. Valid values are 1 to 576.
querier *IP-address*	Configures a snooping querier. The IP address is used as the source in messages. The default is disabled.
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-address*	Configures an interface belonging to a VLAN as a static member of a multicast group. The specified interface is Ethernet or EtherChannel.
source *source-ip-addr*	(Optional) The source IP address for configuring the static-group.

Command Default

The default settings are as follows:

- **explicit-tracking**—enabled
- **fast-leave**—disabled for all VLANs
- **last-member-query-interval**—1 second
- **querier** *IP-address*—disabled
- **report-suppression**—enabled

Send feedback to nexus4K-docfeedback@cisco.com

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

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 192.168.2.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 192.168.2.1 interface ethernet 1/10
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information and configuration.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

LACP must be enabled on the switch.

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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

LACP must be enabled on the switch.

Each device that runs LACP has an LACP system priority value. You can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems.

When setting the priority, note that a *higher* number means a *lower* priority.

Examples

This example shows how to set the LACP system priority for the device to 2500:

```
switch(config)# lacp system-priority 2500
```

Related Commands

Command	Description
show lacp	Displays LACP information.

Send feedback to nexus4K-docfeedback@cisco.com

link debounce

To enable the debounce timer on an interface, use the **link debounce** command. To disable the timer, use the **no** form of this command.

link debounce [**time** *milliseconds*]

no link debounce

Syntax Description

time *milliseconds*	(Optional) Specifies the extended debounce timer. Valid values are from 0 to 5000 milliseconds. A value of 0 milliseconds disables the debounce time.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The port debounce time is the amount of time that an interface waits to notify the supervisor of a link going down. During this time, the interface waits to see if the link comes back up. The wait period is a time when traffic is stopped.

Caution When you enable the debounce timer, link up and link down detections are delayed, resulting in a loss of traffic during the debounce period. This situation might affect the convergence of some protocols.

Examples

The following example shows how to enable the debounce timer and set the debounce time to 1000 milliseconds for an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# link debounce time 1000
```

The following example shows how to disable the debounce timer for an Ethernet interface:

```
switch(config-if)# no link debounce
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send feedback to nexus4K-docfeedback@cisco.com

link state group

To configure a port as a member of a link-state group, use the **link state group** interface configuration command. To remove the port from the link-state group, use the **no** form of this command.

link state group [*number*] {**upstream** | **downstream**}

no link state group [*number*] {**upstream** | **downstream**}

Syntax Description(

number	(Optional) Specifies the link-state group number. The range is from 1 to 6. The default is 1.
upstream	Configures a port as an upstream port for a specific link-state group.
downstream	Configures a port as a downstream port for a specific link-state group.

Command Default

The default group is group 1.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Link-state tracking (LST) must be enabled on the switch.

Use the **link state group** interface configuration command to configure a port as an upstream or downstream interface for the specified link-state group. If the group number is omitted, the default group number is 1.

To enable link-state tracking, create a *link-state group*, and specify the interfaces that are assigned to the link-state group. An interface can be an aggregation of ports (an EtherChannel), a single physical port in access or trunk mode, or a routed port. In a link-state group, these interfaces are bundled together. The *downstream interfaces* are bound to the *upstream interfaces*. Interfaces connected to servers are referred to as downstream interfaces, and interfaces connected to distribution switches and network devices are referred to as upstream interfaces.

For more information about the inters between the downstream and upstream interfaces, see the “Configuring EtherChannels and Link-State Tracking” chapter of the software configuration guide for this release.

Follow these guidelines to avoid configuration problems:

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- An interface cannot be a member of more than one link-state group.
- You can configure only ten link-state groups for each switch.

Send feedback to nexus4K-docfeedback@cisco.com

Examples

This example shows how to configure the interfaces as **upstream** in group 6:

```
switch(config)# feature lst
switch(config)# interface ethernet 1/2
switch(config-if)# link state group 6 upstream
switch(config-if)#
```

This example shows how to remove the interfaces as **upstream** in the group 6 configuration:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no link state group 6 upstream
switch(config-if)#
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
link state track	Enables a link-state group.
show link state group	Displays the link-state group information.
show running-config	Displays the contents of the currently running configuration file.

Send feedback to nexus4K-docfeedback@cisco.com

link state track

To add a link-state tracking (LST) group, use the **link state track** user EXEC command. To remove a link-state group, use the **no** form of this command.

link state track [*number*]

no link state track [*number*]

Syntax Description

number	(Optional) Specify the link-state group number. The group number can be 1 to 6. The default is 1.

Command Default

Link-state tracking is disabled for all groups.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable link-state tracking (LST) on the switch by using the **feature lst** command. The commands for configuring link-state groups are not visible until you enable this feature.

Use the **link state track** global configuration command to create or delete a link-state group.

Examples

This example shows how to enable link-state group 6:

```
switch(config)# link state track 6
switch(config)#
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
feature lst	Enables link-state tracking on a switch.
link state group	Configures an interface as a member of a link-state group.
show link state group	Displays the link-state group information.
show running-config	Displays the contents of the currently running configuration file.

Send feedback to nexus4K-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 1800 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

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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.

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
```

Send feedback to nexus4K-docfeedback@cisco.com

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 feedback to nexus4K-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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

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 feedback to nexus4K-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** [**auto-learn**] | **interface** {**ethernet** *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	Specifies the type of interface.
ethernet *slot*/*port*	Specifies the Ethernet interface slot number and port number in the format 1/1.
port-channel *number*	Specifies the EtherChannel number. Valid values are 1 to 576.
auto-learn	(Optional) Allows moving of this MAC address.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

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

Send feedback to nexus4K-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* [**shut | type local**] | **all shut**}

no monitor session {*number* | **all shut**}

Syntax Description

number	Specifies the SPAN session to create or configure. Use a session number from 1 to 18.
all	Specifies to apply configuration information to all SPAN sessions.
shut	Shuts the selected SPAN session or all SPAN sessions.
type local	(Optional) Creates a local SPAN session.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

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 feedback to nexus4K-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. The name can be 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

No default behavior or values.

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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. The name can be of 32 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

Mst configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 {**destination-ip** | **destination-mac** | **destination-port** | **source-destination-ip** | **source-destination-mac** | **source-destination-port** | **source-ip** | **source-mac** | **source-port**}

no port-channel load-balance ethernet {**destination-ip** | **destination-mac** | **destination-port** | **source-destination-ip** | **source-destination-mac** | **source-destination-port** | **source-ip** | **source-mac** | **source-port**}

Syntax Description

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.

Command Default

Loads distribution on the source and destination MAC address.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the load-balancing method that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in that EtherChannel. Using source addresses or IP addresses might result in better load balancing.

Examples

This example shows how to set the load-balancing method to use the source IP:

```
switch(config)# port-channel load-balance ethernet source-ip
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show port-channel load-balance	Displays information on EtherChannel load balancing.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable private VLANs by using the **feature private-vlan** command before you can configure private VLANs. The commands for configuring private VLANs are not visible until you enable private VLANs.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. When you reconvert the specified VLAN to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. If you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and are reenabled when you recreate the specified VLAN and configure it as the previous secondary VLAN.

You cannot configure VLAN1 or the internally allocated VLANs as private VLANs.

A private VLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

An isolated VLAN is a VLAN that is used by isolated ports to communicate with promiscuous ports. The traffic of an isolated VLAN is blocked on all other private ports in the same VLAN. Its traffic can only be received by standard trunking ports and promiscuous ports that are assigned to the corresponding primary VLAN.

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

Send feedback to nexus4K-docfeedback@cisco.com

A community VLAN is defined as the VLAN that carries the traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

A primary VLAN is defined as the VLAN that is used to convey the traffic from the routers to customer end stations on private ports.

Multiple community and isolated VLANs are allowed. If you enter a range of primary VLANs, the system uses the first number in the range for the association.

Note A PVLAN isolated port on a 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 feedback to nexus4K-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. Valid VLAN IDs range from 1 to 4094.
remove	Clears the association between a secondary VLAN and a primary VLAN.

Command Default

No default behavior or values.

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 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 feedback to nexus4K-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 arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Mst configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 that is not connected to a host can cause a bridging loop because the port ignores any BPDU that it receives, and the port moves to the STP forwarding state.

Use the **spanning-tree port type edge bpdufilter default** command to enable BPDU Filtering on all spanning tree edge ports.

Examples

This example shows how to explicitly enable BPDU Filtering on the Ethernet spanning tree edge port 1/4:

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

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Examples

This example shows how to enable BPDU Guard on this interface:

```
switch(config)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send feedback to nexus4K-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 Table 2-1 for the port cost values).

Command Default

Port cost is set by the media speed.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	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 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 feedback to nexus4K-docfeedback@cisco.com

The EtherChannel 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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 4001I and Cisco Nexus 4005I switch module, 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 feedback to nexus4K-docfeedback@cisco.com

spanning-tree loopguard default

To enable Loop Guard as a default on all spanning tree normal and network ports, use the **spanning-tree loopguard default** command. To disable Loop Guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 {**mst** | **rapid-pvst**}

no spanning-tree mode

Syntax Description

mst	Sets the STP mode to MST.
rapid-pvst	Sets the STP mode to Rapid PVST+.

Command Default

Rapid PVST+.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 arguments or keywords.

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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The port cost depends on the port speed. The faster interface speeds indicate smaller costs. MST always uses long path costs.

Higher cost values indicate higher costs. When entering the cost, do not include a comma in the entry. For example, enter 1000, not 1,000.

The EtherChannel bundle is considered 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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to set the forward-delay timer:

```
switch(config)# spanning-tree mst forward-time 20
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to set the number of possible hops:

```
switch(config)# spanning-tree mst max-hops 25
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send feedback to nexus4K-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 240 in increments of 32.

Command Default

Port priority value is 128.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 permissible values and additional information.

Command Default

Bridge priority default is 32768.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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** [**diameter** *dia* [**hello-time** *hello-time*]] | **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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Send feedback to nexus4K-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 [**disable**]

no spanning-tree mst simulate pvst

Syntax Description

disable	(Optional) Disables PVST simulation on the interface.

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

Command History

Release	Modification
4.1(2)E1(1)	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+ Shared Spanning Tree Protocol (SSTP) bridge protocol data unit (BPDU) move into the STP blocking state. Those interfaces remain in the inconsistent state until the port stops receiving Rapid PVST+ BPDUs, and then the port resumes the normal STP transition process.

Note To block automatic MST and Rapid PVST+ interoperability for the entire switch, use **no spanning-tree mst simulate pvst global** command.

This command is useful when you want to prevent accidental connection with a device running Rapid PVST+.

To reenable seamless operation between MST and Rapid PVST+ on specific interfaces, use the **spanning-tree mst simulate pvst** command.

Send feedback to nexus4K-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 feedback to nexus4K-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 **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 **no spanning-tree mst simulate pvst global** command.

spanning-tree mst simulate pvst global

no spanning-tree mst simulate pvst global

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled. By default, the switch interoperates seamlessly between MST and Rapid PVST+.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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+ Shared Spanning Tree Protocol (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 feedback to nexus4K-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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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
```

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
```

Send feedback to nexus4K-docfeedback@cisco.com

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 feedback to nexus4K-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 arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 functionality of the BPDU Filtering feature is different when you enable it for each port 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 feedback to nexus4K-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 feedback to nexus4K-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 arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 for each interface. For more information, see the **spanning-tree bpduguard** command.

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 feedback to nexus4K-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 feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use this command to automatically configure all interfaces as spanning tree edge ports by default. This command does 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 feedback to nexus4K-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 feedback to nexus4K-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
4.1(2)E1(1)	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 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 feedback to nexus4K-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 for each specified interface.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree configuration.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

spanning-tree vlan

To configure Spanning Tree Protocol (STP) parameters for each VLAN, 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** [**diameter** *dia* [**hello-time** *value*]] | **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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Send feedback to nexus4K-docfeedback@cisco.com

Usage Guidelines

Caution When disabling spanning tree on a VLAN using the **no spanning-tree vlan** *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.

Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When setting the **max-age** *seconds*, if a bridge does not see BPDUs from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

The **spanning-tree root primary** alters the bridge priority of this switch to 24576. If you enter the **spanning-tree root primary** command and the switch does not become the root, 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 feedback to nexus4K-docfeedback@cisco.com

speed (Ethernet)

To configure the transmit and receive speed for an Ethernet interface, use the **speed** command. To reset to the default speed, use the **no** form of this command.

speed {**1000** | **10000** | **auto**}

no speed

Syntax Description

1000	Sets the interface speed to 1-Gigabit.
10000	Sets the interface speed to 10-Gigabit. This is the default speed.
auto	Automatically negotiates the interface speed.

Command Default

The default speed is 10000 (10-Gigabit).

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The first 8 ports of a Nexus 5010 switch and the first 16 ports of a Nexus 5020 switch are switchable 1-Gigabit and 10-Gigabit ports. The default interface speed is 10-Gigabit. To configure these ports for 1-Gigabit Ethernet, insert a 1-Gigabit Ethernet SFP transceiver into the applicable port and then set its speed with the speed command.

Note If the interface and transceiver speed is mismatched, the SFP validation failed message is displayed when you enter the **show interface ethernet** *slot/port* command. For example, if you insert a 1-Gigabit SFP transceiver into a port without configuring the **speed 1000** command, you get this error.

By default, all ports on a switch are 10 Gigabits.

Examples

The following example shows how to set the speed for a 1-Gigabit Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# speed 1000
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

switchport access vlan

To set the access mode of the interface to a specified VLAN, use the **switchport access vlan** command. To reset the access mode of the interface to the default VLAN, 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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the **no** form of the **switchport access vlan** command to reset the access mode of the interface to the default VLAN. This 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 feedback to nexus4K-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
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

switchport mode private-vlan host

To set the interface type to be a host port for a private VLAN, use the **switchport mode private-vlan host** command.

switchport mode private-vlan host

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When you configure a port as a host private VLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid private VLAN association configured.
- The port is a Switched Port Analyzer (SPAN) destination.
- The private VLAN association is suspended.

If you delete a private VLAN port association, or if you configure a private port as a SPAN destination, the deleted private VLAN port association or the private port that is configured as a SPAN destination, 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 feedback to nexus4K-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 arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-host mode. If the port is in private VLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive. The port also may be inactive when the association between the private VLANs is suspended.

The secondary VLAN may be an isolated or community VLAN.

See the **private-vlan** command for more information on primary VLANs, secondary VLANS, and isolated or community ports.

Note A PVLAN isolated port on a 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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show vlan private-vlan	Displays information on private VLANs.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	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 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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

udld (configuration mode)

To configure the Unidirectional Link Detection (UDLD) protocol on the switch, use the **udld** command. To disable UDLD, use the **no** form of this command.

udld {**aggressive** | **message-time** *timer-time* | **reset**}

no udld {**aggressive** | **message-time** | **reset**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on the switch.
message-time *timer-time*	Sets the period of time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional. Valid value is from 7 to 90 seconds. Default value is 15 seconds.
reset	Resets all the ports that are shut down by UDLD and permit traffic to begin passing through them again. Other features, such as spanning tree, behave normally if enabled.

Command Default

UDLD aggressive mode is disabled by default.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you configure the UDLD protocol, make sure that UDLD is enabled on the switch.

You can configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. If UDLD aggressive mode is enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD frames, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

To prevent spanning tree loops, normal UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When you enable the UDLD aggressive mode, the following occurs:

- One side of a link has a port stuck (both transmission and receive)
- One side of a link remains up while the other side of the link is down

In these cases, the UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.

Examples

The following example shows how to enable the aggressive UDLD mode for the switch:

```
switch# configure terminal
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config)# udld aggressive
```

This example shows how to reset all ports that were shutdown by UDLD:

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

Related Commands

Command	Description
feature udld	Enables or disables UDLD on a switch.
show udld	Displays the administrative and operational UDLD status.

Send feedback to nexus4K-docfeedback@cisco.com

udld (Ethernet)

To enable and configure the Unidirectional Link Detection (UDLD) protocol on an Ethernet interface, use the **udld** command. To disable UDLD, use the **no** form of this command.

udld {**aggressive** | **disable** | **enable**}

no udld {**aggressive** | **disable** | **enable**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on the interface.
disable	Disables UDLD on the interface.
enable	Enables UDLD in normal mode on the interface.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure normal or aggressive UDLD modes for an Ethernet interface. Before you can enable a UDLD mode for an interface, make sure that UDLD is enabled on the switch. UDLD must also be enabled on the other linked interface and its device.

To use the normal UDLD mode on a link, you must configure one of the ports for normal mode and configure the port on the other end for the normal or aggressive mode. To use the aggressive UDLD mode, you must configure both ends of the link for aggressive mode.

Examples

The following example shows how to enable the normal UDLD mode for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# udld enable
```

This example shows how to enable the aggressive UDLD mode for an Ethernet port:

```
switch(config-if)# udld aggressive
```

This example shows how to disable UDLD for an Ethernet port:

```
switch(config-if)# udld disable
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
feature udld	Enables or disables UDLD on a switch.
show udld	Displays the administrative and operational UDLD status.

Send feedback to nexus4K-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.

Command Default

No default behavior or values.

Command Modes

Configuration

Note You can also create and delete VLANs in the vlan configuration mode using these same commands.

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

Send feedback to nexus4K-docfeedback@cisco.com



CHAPTER 3

Ethernet show Commands

This chapter describes the Cisco NX-OS Ethernet **show** commands available on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

show cdp

To display the information about Cisco Discovery Protocol (CDP), use the **show cdp** command.

show cdp {**all** | **entry** {**all** | **name** *name*} | **global** | **interface** {**ethernet** *slot* | **mgmt** *mgmt-number*} | **neighbors** [**detail** | **interface** {**ethernet** *slot* | **mgmt** *mgmt-number*}] | **traffic interface** {**ethernet** *slot* | **mgmt** *mgmt-number*}}

Syntax Description

all	Displays all interfaces in the CDP database.
entry	Displays CDP entries in the database.
name	Name of a specific CDP entry. The name can be maximum 256 characters.
global	Displays CDP global parameters.
interface	Displays CDP parameters for an interface.
ethernet *slot*	Specifies an Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
mgmt *mgmt-number*	Specifies a management interface.
neighbors	Displays information about CDP neighbors.
detail	Displays detailed information about a CDP neighbor.
traffic	Displays CDP traffic statistics.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify an interface, the system displays all the MAC addresses.

Examples

The following is sample output from the **show cdp all** command and displays the CDP status information of all interfaces:

```
switch# show cdp all
mgmt0 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
mgmt1 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/1 is down
    CDP enabled on interface
```

Send feedback to nexus4K-docfeedback@cisco.com

```
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/2 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/3 is down
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/4 is down
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/5 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/6 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/7 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/8 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/9 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/10 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
Ethernet1/11 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
switch(config)#
```

The following is sample output from the **show cdp interface ethernet 1/1** command and displays the CDP status information of an interface:

```
switch# show cdp interface ethernet 1/1
Ethernet1/1 is up
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
switch#
```

Related Commands

Command	Description
mac-address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
show mac-address-table	Displays information on the MAC address table.

Send feedback to nexus4K-docfeedback@cisco.com

Send feedback to nexus4K-docfeedback@cisco.com

show interface

To display the status and configuration information of interfaces, use the **show interface** command.

show interface

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Configuration

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can use this command without any arguments or keywords. If you do not specify any arguments or keywords with this command, the system displays the status and configuration information of all available interfaces in the system.

Examples

The following is sample output from the **show interface** command and displays the configuration information of all interfaces:

```
switch# show interface
```

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.
interface port-channel	Configures an EtherChannel interface.
show interface ethernet	Displays the status and configuration information about Ethernet IEEE 802.3 interfaces.
show interface mac-address	Displays the MAC address information of interfaces.
show interface port-channel	Displays the status of EtherChannels.
show interface private-vlan mapping	Displays the status and configuration information about private VLANs.
show interface switchport	Displays switchport information of interfaces.

Send feedback to nexus4K-docfeedback@cisco.com

show interface ethernet

To display the status and configuration information about Ethernet IEEE 802.3 interfaces, use the **show interface ethernet** command.

show interface ethernet *slot*

Syntax Description

slot	Specifies the Ethernet interface slot and port number. The slot number is specified in the format 1/1.

Command Default

No default behavior or values.

Command Modes

Configuration

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must configure Ethernet IEEE 802.3 interfaces by using the **interface ethernet** command.

Examples

The following is sample output from the **show interface ethernet 1/1** command and displays information about the Ethernet interface:

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
  Hardware: 1000/10000 Ethernet, address: 0005.ad00.3560 (bia 0005.ad00.3560)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is access
  full-duplex, 10 Gb/s, media type is 10g
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  Last link flapped 05:20:01
  Last clearing of "show interface" counters never
  1 minute input rate 0 bits/sec, 0 packets/sec
  1 minute output rate 0 bits/sec, 198 packets/sec
  Rx
    3 input packets 1389196402 unicast packets 2538321433 multicast packets
    577310354 broadcast packets 13202600302 jumbo packets 2982637346 storm suppression
packets
    192 bytes
  Tx
    5525913 output packets 10556 multicast packets
    3 broadcast packets 7384081665 jumbo packets
    762673 bytes
```

Send feedback to nexus4K-docfeedback@cisco.com

```
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 132264887 CRC 0 ecc
    0 overrun  0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 26 Tx pause
  1 interface resets

switch#
```

Related Commands

Command	Description
interface ethernet	Enters interface configuration mode for an Ethernet IEEE 802.3 interface.
show interface	Displays status and configuration information about interfaces.
show interface switchport	Displays information about the ports, including those in private VLANs.

Send feedback to nexus4K-docfeedback@cisco.com

show interface mac-address

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

show interface [**ethernet** *slot*] **mac-address**

Syntax Description

ethernet	(Optional) Specifies the Ethernet interface for which MAC addresses should be displayed.
slot	The Ethernet interface slot number and port number. The slot number is specified in the format 1/1.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify an interface, the system displays all the MAC addresses.

Examples

The following is sample output from the **show interface mac-address** command and displays the MAC addresses of all interfaces:

```
switch# show interface mac-address
```

The following is sample output from the **show interface ethernet 1/1 mac-address** command and displays the MAC address information of a specific Ethernet interface:

```
switch# show interface ethernet 1/1 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 interface	Displays status and configuration information of interfaces.
show mac-address-table	Displays information on the MAC address table.

Send feedback to nexus4K-docfeedback@cisco.com

show interface port-channel

To display information about EtherChannel interfaces, use the **show interface port-channel** command.

show interface port-channel *channel-number*

Syntax Description

channel-number	EtherChannel number. The range of valid values is 1 to 576.

Command Default

No default behavior or values.

Command Modes

Configuration

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must configure an EtherChannel group interface using the **interface port-channel** command.

Examples

The following is sample output from the **show interface port-channel 1** command and displays information about the EtherChannel interface:

```
switch# show interface port-channel 1
port-channel1 is down (No operational members)
  Hardware: Port-Channel, address: 0000.0000.0000 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is access
  unknown enum 3-duplex, 10 Gb/s
  Input flow-control is off, output flow-control is off
  Switchport monitor is off
  No members
  Last clearing of "show interface" counters never
  1 minute input rate 0 bits/sec, 0 packets/sec
  1 minute output rate 0 bits/sec, 0 packets/sec
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun  0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
```

Send feedback to nexus4K-docfeedback@cisco.com

```
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause
  0 interface resets

switch#
```

Related Commands

Command	Description
interface port-channel	Creates and configures an EtherChannel interface.
show interface	Displays status and configuration information of interfaces.
show interface switchport	Displays information about the ports, including those in private VLANs.
show port-channel load-balance	Displays information on EtherChannel load balancing.
show port-channel summary	Displays summary information on the EtherChannels.

Send feedback to nexus4K-docfeedback@cisco.com

show interface priority-flow-control

To display the priority flow control (PFC) details for interfaces, use the **show interface priority-flow-control** command.

show interface priority-flow-control

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show interface priority-flow-control** command and displays the priority flow control information of interfaces:

```
switch(config)# show interface priority-flow-control
=======================================

Interface      Admin      Oper(VL bmap)
=======================================

Ethernet1/1 Auto Off
Ethernet1/2 Auto Off
Ethernet1/3 Auto Off
Ethernet1/4 Auto Off
Ethernet1/5 Auto Off
Ethernet1/6 Auto Off
Ethernet1/7 Auto Off
Ethernet1/8 Auto Off
Ethernet1/9 Auto Off
Ethernet1/10 Auto Off
Ethernet1/11 Auto Off
Ethernet1/12 Auto Off
Ethernet1/13 Auto Off
Ethernet1/14 Auto Off
Ethernet1/15 Auto Off
Ethernet1/16 Auto Off
Ethernet1/17 Auto Off
Ethernet1/18 Auto Off
Ethernet1/19 Auto On (8)
Ethernet1/20 Auto Off

switch(config)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
priority-flow-control mode	Configures the priority flow control (PFC) mode on an interface.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Any

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show interface private-vlan mapping** command and displays information about primary and secondary private VLAN mapping:

```
switch# show interface private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan3     2              non-operational
switch#
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
show interface	Displays status and configuration information of interfaces.
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 feedback to nexus4K-docfeedback@cisco.com

show interface switchport

To display switch port information of interfaces, use the **show interface switchport** command.

show interface [**ethernet** *slot* | **port-channel** *number*] **switchport**

Syntax Description

ethernet	(Optional) Specifies the Ethernet interface for which switch port information should be displayed.
slot	The Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
port-channel	(Optional) Specifies the EtherChannel for which switch port information should be displayed.
number	EtherChannel number. Valid values are 1 to 576.

Command Default

No default behavior or values.

Command Modes

Any

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify an Ethernet interface, the system displays the switch port information of all Ethernet interfaces.

You must configure an EtherChannel interface using the **interface port-channel** command before you can display the switch port information of an EtherChannel.

Examples

The following is sample output from the **show interface switchport** command and displays the switch port information for all Ethernet interfaces:

```
switch# show interface switchport
```

The following is sample output from the **show interface ethernet 1/1 switchport** command and displays the switch port information of an Ethernet interface:

```
switch# show interface ethernet 1/1 switchport
Name: Ethernet1/1
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
switch#
```

The following is sample output from the **show interface port-channel 1 switchport** command and displays the switch port information of an EtherChannel:

```
switch# show interface port-channel 1 switchport
Name: port-channel1
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
switch#
```

Related Commands

Command	Description
interface port-channel	Creates and configures an EtherChannel interface.
show interface	Displays status and configuration information of interfaces.
show interface ethernet	Displays information of Ethernet interfaces.
show interface port-channel	Displays information of EtherChannel.
show port-channel summary	Displays summary information on the EtherChannels.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show ip igmp snooping** command and displays information about the IGMP snooping configuration:

```
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 feedback to nexus4K-docfeedback@cisco.com

show lacp

To display Link Aggregation Control Protocol (LACP) information, use the **show lacp** command.

show lacp {**counters** [**interface port-channel** *number*] | **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 port-channel *number*	Specifies an EtherChannel interface. Valid values are 1 to 576.
interface ethernet *slot*/*port*	Displays LACP information for a specific Ethernet interface. The slot number is specified in the format 1/1.
neighbor	Displays information about the LACP neighbor. Optionally provide an EtherChannel number.
port-channel	Displays information about an EtherChannel. Optionally provide an EtherChannel 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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

LACP must be enabled on the switch.

Use the **show lacp** command to troubleshoot problems related to LACP in a network.

Examples

The following is sample output from the **show lacp system-identifier** command and displays information about the LACP system identification:

```
switch# show lacp system-identifier
```

Related Commands

Command	Description
feature lacp	Enables LACP on interfaces.

Send feedback to nexus4K-docfeedback@cisco.com

show link state group

To display the link-state group information, use the **show link state group** privileged EXEC command.

show link state group [*number*] [**detail**] [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

number	(Optional) Number of the link-state group.
detail	(Optional) Specifies that detailed information appears.
begin	(Optional) Displays begins with the line that matches the *expression*.
exclude	(Optional) Displays excludes lines that match the *expression*.
include	(Optional) Displays includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

To display the link-state group information, use the **show link state group** command. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group.

Enter the **detail** keyword to display detailed information about the group. The output for the **show link state group detail** command displays only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces (or both) configured. If there is no link-state configuration for a group, the group is not shown as enabled or disabled.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Send feedback to nexus4K-docfeedback@cisco.com

Examples

The following is sample output from the **show link state group 1** command and displays information about a specific link-state group:

```
switch# show link state group 1
Link State Group: 1      Status: Enabled, Down
```

The following is sample output from the **show link state group detail** command and displays detailed information about the link-state groups:

```
switch# show link state group detail
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi1/0/17(Dwn) Gi1/0/18(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
switch#
```

Related Commands

Command	Description
feature lst	Enables link-state tracking (LST).
link state group	Configures an interface as a member of a link-state group.
link state track	Enables a link-state group.
show running-config	Displays the operating configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show mac-address-table aging-time** command and displays information about 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 feedback to nexus4K-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** [**interface** {**ethernet** *slot/port* | **port-channel** *number*}] | **static** [**interface** {**ethernet** *slot/port* | **port-channel** *number*}] | **vlan** *vlan-id*]

Syntax Description

address *EEEE.EEEE.EEEE*	(Optional) Displays a count of the MAC address table entries for a specific address.
dynamic	(Optional) Displays a count of the dynamic MAC addresses.
static	(Optional) Displays a count of the static MAC addresses.
interface	(Optional) Specifies the type of interface, Ethernet or EtherChannel.
ethernet *slot/port*	Specifies the Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
port-channel *number*	Specifies the EtherChannel number.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN. The range of valid values is from 1 to 4094.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show mac-address-table count dynamic** command and displays information about 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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show mac-address-table notification mac-move** command and displays information about 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 feedback to nexus4K-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, the slot number, and the port number, or the EtherChannel number. The slot number is specified in the format 1/1.
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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show mac-address-table** command and displays information about the entries for the MAC address table:

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

The following is sample output from the **show mac-address-table address** command and displays information about the entries for the MAC address table for a specific MAC address:

```
switch# show mac-address-table address 0018.bad8.3fbd
```

The following is sample output from the **show mac-address-table dynamic** command and displays information about the dynamic entries of the MAC address table:

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

Send feedback to nexus4K-docfeedback@cisco.com

The following is sample output from the **show mac-address-table interface ethernet 1/3** command and displays information about the MAC address table for a specific interface:

```
switch# show mac-address-table interface ethernet 1/3
```

The following is sample output from the **show mac-address-table static** command and displays information about the static entries in the MAC address table:

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

The following is sample output from the **show mac-address-table vlan 5** command and displays information about 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 feedback to nexus4K-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**]]

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.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must configure a session in the system using the **monitor session** command before you can use this command.

Examples

The following is sample output from the **show monitor session 1** command and displays information about an SPAN session:

```
switch# show monitor session 1
```

The following is sample output from the **show monitor session range 1-4** command and displays information about 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 feedback to nexus4K-docfeedback@cisco.com

show port-channel load-balance

To display information on EtherChannel load balancing, use the **show port-channel load-balance** command.

show port-channel load-balance

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Configuration

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show port-channel load-balance** command and displays information about EtherChannel load balancing:

```
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#
```

Related Commands

Command	Description
port-channel load-balance ethernet	Sets the load-balancing method for the EtherChannels.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Configuration

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must configure an EtherChannel group using the **interface port-channel** command.

Examples

The following is sample output from the **show port-channel summary** command and displays summary information about EtherChannels:

```
switch# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
--------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------
1     Po1(SD)     Eth      NONE      --

switch#
```

Related Commands

Command	Description
interface port-channel	Configures EtherChannel interfaces.
show interface port-channel	Displays information on traffic on the specified EtherChannel interfaces.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config** command and displays information about the running configuration:

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

The following is sample output from the **show running-config all** command and displays detailed information about the running configuration:

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

Related Commands	Command	Description
	show startup-config	Displays the contents of the startup configuration file.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The output of this command varies depending on whether you are running Rapid PVST+ or MST.

Examples

The following is sample output from the **show running-config spanning-tree** command and displays information about the running STP configuration:

```
switch# show running-config spanning-tree
```

The following is sample output from the **show running-config spanning-tree all** command and displays information about the running STP configuration:

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

Related Commands

Command	Description
show spanning-tree	Displays information about STP.

Send feedback to nexus4K-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 4094.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command provides information on the specified VLAN, including private VLANs.

The output of this command varies with your configuration. If you have configured the VLAN name, shutdown status, or suspended status, these are also displayed.

Examples

The following is sample output from the **show running-config vlan 5** command and displays information about the running configuration of a VLAN:

```
switch# show running-config vlan 5
```

Related Commands

Command	Description
show vlan	Displays information about all the VLANs on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

show solm cin

To display the Chassis Internal Network (CIN) VLAN configuration status, use the **show solm cin** command.

show solm cin

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must configure CIN VLANs using the **cin** command before you use this command.

Examples

The following is sample output from the **show solm cin** command and displays information about the CIN VLAN status:

```
switch # show solm cin
20-24,26-33,100
switch #
```

Related Commands

Command	Description
cin	Configures CIN VLANs.
show solm counters	Displays the Ingress and Egress counters for CIN VLANs.

Send feedback to nexus4K-docfeedback@cisco.com

show solm counters

To display the Ingress and Egress counters for interfaces, use the **show solm counters** command.

show solm counters [**interface** {**ethernet** *slot/port* | **mgmt** *mgmt-port*}]

Syntax Description

interface	(Optional) Display counters for an interface.
ethernet	Specifies an Ethernet IEEE 802.3 interface.
slot/port	Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
mgmt	Specifies a management interface.
mgmt-port	Management interface number.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The output of the **show solm counters** command varies depending on the CIN traffic for each interface.

Examples

The following is sample output from the **show solm counters** command and displays information about the CIN VLAN counters for all interfaces:

```
switch# show solm counters

------------------------------------------------------------------------
Interface           TX-UCast      TX-MCast      RX-UCast      RX-MCast
------------------------------------------------------------------------

mgmt1               0             0             0             0
Ethernet1/1         0             0             0             0
Ethernet1/2         0             0             0             0
Ethernet1/3         0             0             0             0
Ethernet1/4         0             0             0             0
Ethernet1/5         0             0             0             0
Ethernet1/6         0             0             0             0
Ethernet1/7         0             0             0             0
Ethernet1/8         0             0             0             0
Ethernet1/9         0             0             0             0
Ethernet1/10        0             0             0             0
Ethernet1/11        0             0             0             0
Ethernet1/12        0             0             0             0
Ethernet1/13        0             0             0             0
Ethernet1/14        0             0             0             0
switch #
```

Send feedback to nexus4K-docfeedback@cisco.com

The following is sample output from the **show solm counters interface ethernet 1/1** command and displays information about the CIN VLAN counters of an interface:

```
switch# show solm counters interface ethernet 1/1

--------------------------------------------------------------------------
Interface           TX-UCast      TX-MCast      RX-UCast      RX-MCast
--------------------------------------------------------------------------

Ethernet1/1         0             0             0             0
switch#
```

Related Commands

Command	Description
cin	Configures CIN VLANs.
show solm cin	Displays information about the CIN VLANs.

Send feedback to nexus4K-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 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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show spanning-tree** command and displays information about the spanning tree:

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

The following is sample output from the **show spanning-tree blockedports** command and displays the blocked ports in spanning tree:

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

The following is sample output from the **show spanning-tree inconsistentports** command and displays the ports that are in any STP-inconsistent state:

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

The following is sample output from the **show spanning-tree pathcost method** command and displays the path cost method:

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

Send feedback to nexus4K-docfeedback@cisco.com

Table 3-1 describes the fields that are displayed in the output of **show spanning-tree** commands.

Table 3-1 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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

show spanning-tree active

To display spanning-tree protocol (STP) information on STP-active interfaces only, use the **show spanning-tree active** command.

show spanning-tree active [**brief** | **detail**]

Syntax Description

brief	(Optional) Displays a brief summary of STP interface information.
detail	(Optional) Displays a detailed summary of STP interface information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree active** command and displays the STP information about the STP-active interfaces:

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

Related Commands

Command	Description
show spanning-tree	Displays STP information.
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.
show spanning-tree summary	Displays summary information about STP.
show spanning-tree vlan	Displays STP information for specified VLANs.

Send feedback to nexus4K-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 spanning-tree protocol (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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree bridge** command and displays 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 feedback to nexus4K-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 feedback to nexus4K-docfeedback@cisco.com

show spanning-tree brief

To display a brief summary of the spanning-tree protocol (STP) status and configuration on the switch, use the **show spanning-tree brief** command.

show spanning-tree brief [**active**]

Syntax Description

active	(Optional) Displays information about STP active interfaces only.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree brief** command and displays a brief summary of the STP status:

```
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.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree detail

To display detailed information on the spanning-tree protocol (STP) status and configuration on the switch, use the **show spanning-tree detail** command.

show spanning-tree detail [**active**]

Syntax Description

active	(Optional) Displays information about STP active interfaces only.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree detail** command and displays detailed STP information about 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.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree interface

To display information on the spanning-tree protocol (STP) interface status and configuration of specified interfaces, use the **show spanning-tree interface** command.

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

Syntax Description

ethernet *slot*	Specifies the Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
port-channel *number*	Specifies the EtherChannel 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	(Optional) Current port STP state.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Examples

The following is sample output from the **show spanning-tree interface ethernet 1/3** command and displays STP information about a specified interface:

```
switch(config)# show spanning-tree interface ethernet 1/3
```

The following is sample output from the **show spanning-tree interface ethernet 1/3 detail** command and displays detailed STP information about 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 brief	Displays brief summary information about STP.
show spanning-tree detail	Displays detailed information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree mst

To display information on Multiple Spanning Tree (MST) status and configuration, use the **show spanning-tree mst** command.

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

Syntax Description

instance-id	(Optional) The MST instance range that you want to display. For example, 0-3, 5, 7-9.
detail	(Optional) Displays detailed MST information.
interface	(Optional) Specifies the type of interface.
ethernet *slot/port*	Ethernet interface slot and port number. The slot number is specified in the format 1/1.
port-channel *number*	EtherChannel number. Valid values are 1 to 576.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If the switch is not running in spanning-tree protocol (STP) MST mode when you enter this command, it returns the following message:

```
ERROR: Switch is not in mst mode
```

Examples

The following is sample output from the **show spanning-tree mst** command and displays STP information about MST instance information for the VLAN ports that are currently active:

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

The following is sample output from the **show spanning-tree mst 0** command and displays STP information about a specific MST instance:

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

The following is sample output from the **show spanning-tree mst 0 detail** command and displays STP information about a a specific MST instance:

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

The following is sample output from the **show spanning-tree mst 0 interface ethernet 1/2** command and displays STP interface information about a specific MST instance:

Send feedback to nexus4K-docfeedback@cisco.com

```
switch)# show spanning-tree mst 0 interface ethernet 1/2
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree mst configuration

To display current Multiple Spanning-Tree (MST) regional information including the VLAN-to-instance mapping of all VLANs, use the **show spanning-tree mst configuration** command.

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

Syntax Description

digest	(Optional) Displays information about the MD5 digest.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If the switch is not running in spanning-tree protocol (STP) MST mode when you enter this command, it returns the following message:

```
ERROR: Switch is not in mst mode
```

Examples

The following is sample output from the **show spanning-tree mst configuration** command and displays information about the MST configuration:

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

The following is sample output from the **show spanning-tree mst configuration digest** command and displays the MD5 digest included in the current MST configuration:

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

See Table 3-1 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 summary	Displays summary information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree mst detail

To display detailed information on Multiple Spanning-Tree (MST) status and configuration, use the **show spanning-tree mst detail** command.

show spanning-tree mst detail

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If the switch is not running in spanning-tree protocol (STP) MST mode when you enter this command, it returns the following message:

```
ERROR: Switch is not in mst mode
```

Examples

The following is sample output from the **show spanning-tree mst detail** command and displays the detailed STP information about the MST protocol:

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

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree summary	Displays summary information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree mst interface

To display Multiple Spanning-Tree (MST) interface status and configuration information, use the **show spanning-tree mst interface** command.

show spanning-tree mst interface {**ethernet** *slot/port* | **port-channel** *number*}

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface slot and port number in the format 1/1.
port-channel *number*	Specifies the EtherChannel number. Valid values are 1 to 576.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If the switch is not running in spanning-tree protocol (STP) MST mode when you enter this command, it returns the following message:

```
ERROR: Switch is not in mst mode
```

Examples

The following is sample output from the **show spanning-tree mst interface ethernet 1/2** command and displays MST information about the specified MST interface:

```
switch)# show spanning-tree mst interface ethernet 1/2
```

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree summary	Displays summary information about STP.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree root** command and displays information for the root bridge:

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

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree summary	Displays summary information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree summary

To display summary spanning-tree protocol (STP) information on the switch, use the **show spanning-tree summary** command.

show spanning-tree summary [**totals**]

Syntax Description

totals	(Optional) Displays totals only of STP information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The display output for this command differs when you are running Rapid PVST+ or MST.

Examples

The following is sample output from the **show spanning-tree summary** command and displays summary STP information:

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

Related Commands

Command	Description
show spanning-tree	Displays information STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan

To display spanning-tree protocol (STP) information for specified VLANs, use the **show spanning-tree vlan** command.

show spanning-tree vlan {*vlan-id*} [**blockedports** | **inconsistentports**]

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display. Valid values are 1 to 4094.
blockedports	(Optional) Displays the STP alternate ports in the blocked state for the specified VLANs.
inconsistentports	(Optional) Displays the ports that are in an inconsistent STP state for specified VLANs.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1** command and displays STP information of an interface:

```
switch# show spanning-tree vlan 1
```

The following is sample output from the **show spanning-tree vlan 1 inconsistentports** command and displays information about the inconsistent ports on the interface:

```
switch# show spanning-tree vlan 1 inconsistentports
```

Related Commands

Command	Description
show spanning-tree	Displays information STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan active

To display spanning-tree protocol (STP) information for VLANs and active ports, use the **show spanning-tree vlan active** command.

show spanning-tree vlan {*vlan-id*} **active** [**brief** | **detail**]

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display.
brief	(Optional) Displays brief summary of STP information for the specified VLANs.
detail	(Optional) Displays detailed STP information for the specified VLANs.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 active** command and displays information about the active ports on an interface:

```
switch# show spanning-tree vlan 1 active
```

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree active	Displays information about STP active interfaces only.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan bridge

To display spanning-tree protocol (STP) status and configuration of the bridge for the specified VLANs, use the **show spanning-tree vlan bridge** command.

show spanning-tree vlan {*vlan-id*} **bridge** [**address** | **brief** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display.
address	(Optional) Displays the MAC address for the specified STP bridge for the specified VLANs.
brief	(Optional) Displays brief summary of STP information for the specified VLANs.
detail	(Optional) Displays detailed STP information 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.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 bridge** command and displays STP bridge information of a specified interface:

```
switch# show spanning-tree vlan 1 bridge
```

The following is sample output from the **show spanning-tree vlan 1 bridge address** command and displays information about the MAC address of the bridge on a specified interface:

```
switch# show spanning-tree vlan 1 bridge address
VLAN0001         0005.ad00.3576
switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

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.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan brief

To display a brief summary of spanning-tree protocol (STP) information for specified VLANs, use the **show spanning-tree vlan brief** command.

show spanning-tree vlan {*vlan-id*} **brief** [**active**]

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display. Valid values are 1 to 4094.
active	(Optional) Displays information about STP VLANs and active ports.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 brief** command and displays a brief summary of the STP information of a specified interface:

```
switch# show spanning-tree vlan 1 brief

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0005.ad00.3576
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0005.ad00.3576
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Eth1/1           Desg FWD 2         128.129  P2p
Eth1/2           Desg FWD 2         128.130  P2p
Eth1/6           Desg FWD 2         128.134  P2p
Eth1/8           Desg FWD 2         128.136  P2p
Eth1/15          Desg FWD 2         128.143  P2p
Eth1/16          Desg FWD 2         128.144  P2p
Eth1/17          Desg FWD 2         128.145  P2p
Eth1/18          Desg FWD 2         128.146  P2p
switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree brief	Displays brief summary information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan detail

To display detailed spanning-tree protocol (STP) information for specified VLANs, use the **show spanning-tree vlan detail** command.

show spanning-tree vlan {*vlan-id*} **detail** [**active**]

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display. Valid values are 1 to 4094.
active	(Optional) Displays information about STP VLANs and active ports.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 detail** command and displays detailed information about a specified interface:

```
switch# show spanning-tree vlan 1 detail
```

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree detail	Displays detailed information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan interface

To display spanning-tree protocol (STP) interface status and configuration information for specified VLANs, use the **show spanning-tree vlan interface** command.

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

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display. Valid values are 1 to 4094.
ethernet *slot/port*	Specifies the Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
port-channel *number*	Specifies the EtherChannel number. Valid values are 1 to 576.
active	(Optional) Displays information about STP VLANs and active ports.
brief	(Optional) Displays brief summary of STP information for the specified VLANs.
cost	(Optional) Displays the STP path cost for the specified VLANs.
detail	(Optional) Displays detailed STP information for the specified VLANs.
edge	(Optional) Displays the STP-type edge port information for the specified interface for the specified VLANs.
inconsistency	(Optional) Displays the STP port inconsistency state for the specified interface for the specified VLANs.
priority	(Optional) Displays the STP priority for the specified VLANs.
rootcost	(Optional) Displays the path cost to the root for specified interfaces for the specified VLANs.
state	(Optional) Current port STP state. Valid values are blocking, disabled, learning, and forwarding.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 interface ethernet 1/1** command and displays information about the STP status of an interface:

```
switch# show spanning-tree vlan 1 interface ethernet 1/1
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree interface	Displays STP interface status and configuration of specified interfaces.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan root

To display spanning-tree protocol (STP) status and configuration information of the root bridge for specified VLANs, use the **show spanning-tree vlan root** command.

show spanning-tree vlan {*vlan-id*} **root** [**address** | **brief** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display. Valid values are 1 to 4094.
address	(Optional) Displays the MAC address for the specified STP bridge for the specified VLANs.
brief	(Optional) Displays brief summary of STP information for the specified VLANs.
cost	(Optional) Displays the STP path cost for the specified VLANs.
detail	(Optional) Displays detailed STP information 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.
port	(Optional) Displays information about the root port 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.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 root** command and displays STP status information of the root bridge on a VLAN:

```
switch# show spanning-tree vlan 1 root
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree root	Displays status and configuration of the root bridge for the STP instance to which this switch belongs.

Send feedback to nexus4K-docfeedback@cisco.com

show spanning-tree vlan summary

To display summary spanning-tree protocol (STP) information for specified VLANs, use the **show spanning-tree vlan** command.

show spanning-tree vlan {*vlan-id*} **summary**

Syntax Description

vlan-id	Specifies the VLAN or range of VLANs that you want to display. Valid values are 1 to 4094.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show spanning-tree vlan 1 summary** command and displays summary STP information for a specific VLAN:

```
switch# show spanning-tree vlan 1 summary
```

Related Commands

Command	Description
show spanning-tree	Displays information STP.
show spanning-tree summary	Displays summary information about STP.

Send feedback to nexus4K-docfeedback@cisco.com

show udld

To display information about the Cisco-proprietary Unidirectional Link Detection (UDLD) protocol, use the **show udld** command.

show udld {**ethernet** *slot/port* | **global** | **neighbors**}

Syntax Description

ethernet	Displays UDLD information of a specific Ethernet interface.
slot/port	Ethernet interface slot number and port number. The slot number is specified in the format 1/1.
global	Displays UDLD global status and configuration on all interfaces.
neighbors	Displays UDLD neighbor interfaces.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

UDLD must be enabled on a switch.

Examples

The following is sample output from the **show udld global** command and displays information about the UDLD protocol:

```
switch# show udld global

UDLD global configuration mode: enabled
UDLD global message interval: 15
switch config)#
```

Related Commands

Command	Description
feature udld	Enables or disables UDLD on a switch.
show running-config	Displays the contents of the currently running configuration file.

Send feedback to nexus4K-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. The name can be maximum 32 characters.
summary	(Optional) Displays the number of existing VLANs on the switch.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Examples

The following is sample output from the **show vlan** command and displays information about all VLANs on the switch:

```
switch# show vlan
```

The following is sample output from the **show vlan brief** command and displays a brief information about the VLAN name, status, and associated ports:

```
switch# show vlan brief
```

The following is sample output from the **show vlan name test** command and displays information about the VLAN information for a specific VLAN:

```
switch# show vlan name test
```

The following is sample output from the **show vlan summary** command and displays 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 feedback to nexus4K-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. Valid values are 1 to 4094.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show vlan id 5** command and displays information about the specified VLAN:

```
switch# show vlan id 5
```

Related Commands

Command	Description
show vlan	Displays information about VLANs on the switch.

Send feedback to nexus4K-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. Valid VLAN ID values are 1 to 4094.
type	(Optional) Displays the private VLAN type (primary, isolated, or community).

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Private VLANs must be enabled on the switch.

Examples

The following is sample output from the **show vlan private-vlan** command and displays the private VLANs configured on the switch:

```
switch(config)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ----------
3                   primary
         4          community
switch(config)#
```

The following is sample output from the **show vlan id 4 private-vlan** command and displays the private VLANs on a specified VLAN:

```
switch(config)# show vlan id 4 private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------
         4          community
switch(config)#
```

The following is sample output from the **show vlan private-vlan type** command and displays the types of private VLANs configured on the switch:

```
switch(config)# show vlan private-vlan type
Vlan Type
---- -----------------
3    primary
4    community
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config)#
```

The following is sample output from the **show vlan id 4 private-vlan type** command and displays the type of private VLAN on a specified VLAN:

```
switch(config)# show vlan id 4 private-vlan type
Vlan Type
---- -----------------
4    community
switch(config)#
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
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 feedback to nexus4K-docfeedback@cisco.com

CHAPTER 4

Quality of service Commands

This chapter describes the Cisco NX-OS quality of service commands available on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

bandwidth (QoS)

To allocate a minimum percentage of the interface bandwidth to a queue and configure the bandwidth on both ingress and egress queues, use the **bandwidth** command. To remove a bandwidth configuration, use the **no** form of this command.

bandwidth {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **percent** *percent*}

no bandwidth {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **percent** *percent*}

Syntax Description

rate	Bandwidth rate. The range is from 1 to 10000000000.
bps	(Optional) Specifies the units of bits per second.
kbps	(Optional) Specifies the units of kilobits per second.
mbps	(Optional) Specifies the units of megabits per second.
gbps	(Optional) Specifies the units of gigabits per second.
percent	Specifies the percentage of bandwidth of the underlying link rate.
percent	Percent value in the range from 1 to 100.

Command Default

Default bandwidth rate is kbps.

Command Modes

Policy map type queuing class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You use the system-defined ingress or egress queue class for the type of module to which you want to apply the policy map (see Table 4-1).

Table 4-1 System-Defined Type queuing Class Maps

Class Map Queue Name	Description	Default CoS Values
10-Gigabit Module Egress: 1 strict priority queue and 7 normal queues with 4 thresholds per queue		
1p7q4t-out-pq1 [1]	Egress priority queue of 1p7q4t type	1
1p7q4t-out-q2	Egress queue 2 of 1p7q4t type	2
1p7q4t-out-q3	Egress queue 3 of 1p7q4t type	0
1p7q4t-out-q4	Egress queue 4 of 1p7q4t type	4
1p7q4t-out-q5	Egress queue 5 of 1p7q4t type	5
1p7q4t-out-q6	Egress queue 6 of 1p7q4t type	6

Send feedback to nexus4K-docfeedback@cisco.com

Table 4-1 System-Defined Type queuing Class Maps (continued)

Class Map Queue Name	Description	Default CoS Values
1p7q4t-out-q7	Egress queue 7 of 1p7q4t type	7
1p7q4t-out-q-default	Egress default queue of 1p7q4t type	3

Note After you use this command in a specified policy map, you cannot use the **priority** or **shape** command in the same policy map.

This command does not require a license.

Examples

This example shows how to specify a bandwidth rate for a queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# bandwidth 10 mbps
```

This example shows how to remove a bandwidth rate for a queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# no bandwidth 10 mbps
```

Related Commands

Command	Description
bandwidth remaining	Configures the bandwidth remaining on the interface in a queue.
show class-map	Displays class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

bandwidth remaining

To configure the percentage of the bandwidth remaining on the interface after other allocations are configured on both ingress and egress queues, use the **bandwidth remaining** command. To remove the remaining bandwidth allocation, use the **no** form of this command.

bandwidth remaining percent {*percent*}

no bandwidth remaining percent {*percent*}

Syntax Description

percent	Specifies the percentage of bandwidth of the underlying link rate.
percent	Specifies use of percentage of remaining bandwidth on the underlying link. Valid values are from 0 to 100.

Command Default

No default behavior or values.

Command Modes

Policy map type queuing class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You use the system-defined ingress or egress queue class for the type of module to which you want to apply the policy map (see Table 4-1). You can use this command in conjunction with the **priority** command.

This command does not require a license.

Examples

This example shows how to set the bandwidth remaining for the specified queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# bandwidth remaining percent 25
```

This example shows how to remove the bandwidth remaining for the specified queue:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# no bandwidth remaining percent 25
```

Related Commands

Command	Description
bandwidth	Allocates a minimum percentage of the interface bandwidth to a queue.
show class-map	Displays class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

class

To add a reference to an existing qos class map in a policy map and enter the class mode, use the **class** command. To remove a class from the policy map, use the **no** form of this command.

class [**type qos**] *class-map-name*

no class *class-map-name*

Syntax Description

type qos	(Optional) Specifies the component type, which is qos for this class. By default, the type is qos.
class-map-name	Reference to a class map.

Command Default

No default behavior or values.

Command Modes

Policy map type qos configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

This command does not require a license.

Examples

This example shows how to add a reference to a class map at the end of a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)#
```

This example shows how to add a reference to the class-default class map in a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class class-default
switch(config-pmap-c-qos)#
```

This example shows how to remove a class map reference in a policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# no class traffic_class1
switch(config-pmap-qos)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show class-map type qos	Displays type qos class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

class type network-qos

To add a reference to an existing network QoS class map in a policy map and enter the class mode, use the **class type network-qos** command. To remove a class from the policy map, use the **no** form of this command.

class type network-qos *class-map-name*

no class type network-qos *class-map-name*

Syntax Description

class-map-name	Reference to a class map.

Command Default

No default behavior or values.

Command Modes

Policy map type network-qos configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

This command does not require a license.

Examples

This example shows how to add a reference to a class map in a type network-qos policy map:

```
switch(config)# policy-map type network-qos nqos_policy
switch(config-pmap-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-pmap-nq-c)#
```

This example shows how to remove a class map reference in a type network-qos policy map:

```
switch(config)# policy-map type network-qos nqos_policy
switch(config-pmap-pmap-nq)# no class type network-qos nqos_class
switch(config-pmap-pmap-nq)#
```

Related Commands

Command	Description
show class-map type network-qos	Displays type network-qos class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

class type queuing

To add a reference to an existing queuing class map in a policy map and enter the class mode, use the **class type queuing** command. To remove a class from the policy map, use the **no** form of this command.

class type queuing *class-map-name*

no class type queuing *class-map-name*

Syntax Descriptionn

class-map-name	Reference to a system-defined queuing class map. For a list of the system-defined type queuing class maps, see Table 4-1.

Command Default

No default behavior or values.

Command Modes

Policy map type queuing configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

This command does not require a license.

Examples

This example shows how to add a reference to a class map in a type queuing policy map:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# class type queuing 1p7q4t-out-q3
switch(config-pmap-c-que)#
```

This example shows how to remove a class map reference in a type queuing policy map:

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)# no class type queuing 1p7q4t-out-q3
switch(config-pmap-que)#
```

Related Commands

Command	Description
show class-map type queuing	Displays the type queuing class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

class-map type network-qos

To create or modify a class map that defines a network QoS class of traffic and enter the class-map configuration mode, use the **class-map type network-qos** command. To remove a class map, use the **no** form of this command.

class-map type network-qos *class_map_name*

no class-map type network-qos *class_map_name*

Syntax Description

type network-qos	Specifies the component type network QoS for the class map.
class-map-name	Name assigned to the class map. The name class-default is reserved. The name can be maximum 40 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Class maps of type network qos support only the **match cos** command.

Examples

This example shows how to create or modify a network qos class map:

```
switch(config)# class-map type network-qos my_class1
switch(config-cmap-nq)#
```

This example shows how to remove a network qos class map:

```
switch(config-cmap-nq)# no class-map my_class1
switch(config)#
```

Related Commands

Command	Description
match cos	Defines a traffic class that matches the Class of Service (CoS) values.
show class-map type queuing	Displays class maps.

Send feedback to nexus4K-docfeedback@cisco.com

class-map type qos

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

class-map [**type qos**] {[**match-any** | **match-all**] | *class-map-name*}

no class-map [**type qos**] {[**match-any** | **match-all**] | *class-map-name*]}

Syntax Description

type qos	(Optional) Specifies the component type qos for the class map. By default, the class map type is qos.
match-any	Specifies that if the packet matches any of the criteria configured for this class map with the **match** command, then this class map is applied to the packet.
match-all	Specifies that if the packet matches all the criteria configured for this class map with the **match** command, then this class map is applied to the packet. This is the default action if **match-any** is not specified. **Note** This option does not work. The match criteria is always treated as *match-any*.
class-map-name	Name assigned to the class map. The name class-default is reserved. The name can be maximum 40 characters.

Command Default

The default is class-map type qos.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You cannot delete system-defined queuing class map names. See the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide* for more information on this command.

Note When you configure match all for a QoS class map by entering the *class-map type qos match-all* command, the match-all option does not work. Instead, the match criteria is always treated as match any.

This command does not require a license.

Examples

This example shows how to create or modify a qos class map:

```
switch(config)# class-map my_class1
switch(config-cmap-qos)#
```

Send feedback to nexus4K-docfeedback@cisco.com

This example shows how to remove a qos class map:

```
switch(config-cmap-qos)# no class-map my_class1
switch(config)#
```

Related Commands

Command	Description
match access-group	Defines a traffic class that matches the characteristics of a predefined access control list (ACL).
match class-map	Defines a traffic class that matches the match criteria specified in a predefined class map.
match cos	Defines a traffic class that matches the specified CoS values.
show class-map type qos	Displays all QoS class maps.

Send feedback to nexus4K-docfeedback@cisco.com

class-map type queuing match-any

To modify a queuing type class map and enter the class-map configuration mode, use the **class-map type queuing match-any** command.

class-map type queuing match-any *queuing-class-map-name*

Syntax Description

queuing-class-map-name	Specifies a system-defined queuing class map name. See Table 4-1 for the list of system-define queuing class maps.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If the packet matches any of the criteria configured for this class map with the **match** command, then this class map is applied to the packet. Class maps of type queuing support only this option.

If you modify the queuing type class maps, the configuration for all ports of the specified port type on all virtual device contexts (VDCs) also changes.

You cannot delete the system-defined queuing class map names. See the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide* for more information on using this command.

This command does not require a license.

Examples

This example shows how to modify a queuing class map:

```
switch(config)# class-map type queuing match-any 2q4t-in-q1
switch(config-cmap-que)#
```

Related Commands

Command	Description
match class-map	Defines a traffic class based on the match criteria specified in a predefined class map.
match cos	Defines a traffic class that matches the specified CoS values.
show class-map type queuing	Displays class maps.

Send feedback to nexus4K-docfeedback@cisco.com

clear qos statistics

To clear QoS statistics for type qos packet counters, use the **clear qos statistics** command.

clear qos statistics [{**interface** {**ethernet** *slot* | **port-channel** *number*}} [**input** | **output**] [**type** {**qos** | **queuing**}]]

Syntax Description

interface	(Optional) Specifies the type of interface to clear.
ethernet *slot*	(Optional) Specifies the Ethernet interface slot and port number. The range is from 1 to 1.
port-channel *number*	(Optional) Specifies the EtherChannel number. Valid values are from 1 to 576.
input	(Optional) Clears only input statistics.
output	(Optional) Clears only output statistics.
type	(Optional) Specifies the type of statistics to clear.
qos	Specifies clearing qos statistics.
queuing	Specifies clearing queuing statistics.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify the interface, the device clears the counters for all interfaces.

This command does not require a license.

Examples

This example shows how to clear all QoS statistics:

```
switch# clear qos statistics
```

This example shows how to clear all input QoS statistics for Ethernet 1/1:

```
switch# clear qos statistics interface ethernet 1/1 input
```

Related Commands

Command	Description
qos statistics	Enables or disables QoS statistics.

Send feedback to nexus4K-docfeedback@cisco.com

clear statistics device all

To clear all queuing counters including other non-QoS packet counters, use the **clear statistics device all** command.

clear statistics device all

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **clear statistics device all** command clears the statistics for type queuing counters and interface counters on all devices.

Examples

This example shows how to clear the statistics on all devices:

```
switch# clear statistics device all
```

Related Commands

Command	Description
clear qos statistics	Clears the policy statistics for type qos packet counters.
qos statistics	Enables or disables QoS statistics.

Send feedback to nexus4K-docfeedback@cisco.com

congestion-control

To enable or disable network traffic congestion control at common network bottlenecks, use the **congestion-control** command. To remove the congestion control, use the **no** form of this command.

congestion-control random-detect

no congestion-control random-detect

Syntax Description

random-detect	Enable weighted random early detection (WRED) on a class of traffic. The system randomly drops packets when there is network traffic congestion.

Command Default

By default, WRED is off.

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

WRED monitors traffic in a class or interface and drops packets to avoid congestion. However, if a traffic congestion occurs, WRED does not control the congestion.

Examples

This example shows how to configure congestion control on a type network-qos policy map:

```
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)# class type network-qos my_class1
switch(config-pmap-nq-c)# congestion-control random-detect
switch(config-pmap-nq-c)#
```

Related Commands

Command	Description
class type network-qos	References an existing network-qos class map in a policy map.
policy-map	Creates or modifies policy maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

description

To add a description to a class map, policy map, or table map, use the **description** command. To remove the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

text	Description for the class map, policy map, or table map. The description has a maximum of 200 characters.

Command Default

No default behavior or values.

Command Modes

Class map type qos configuration

Policy map type qos configuration

Policy map type queuing configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add a description to a qos class map:

```
switch(config)# class-map my_class1
switch(config-cmap-qos)# description This class map filters packets that matches an ACL
switch(config-cmap-qos)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

match access-group

To identify a specified access control list (ACL) group as a match criteria for a class map, use the **match access-group** command in the class map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group name *acl-name*

no match access-group name *acl-name*

Syntax Description

name	Matches the characteristics of the predefined access control list (ACL).
acl-name	Name of the ACL. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Class-map type qos configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Note The **permit** and **deny** ACL keywords do not affect the matching of packets.

This command does not require a license.

Examples

This example shows how to create a qos class map that matches characteristics of the ACL my_acl:

```
switch(config)# class-map class_acl
switch(config-cmap-qos)# match access-group name my_acl
```

This example shows how to remove the ACL match criteria from a qos class map:

```
switch(config-cmap-qos)# no match access-group name my_acl
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send feedback to nexus4K-docfeedback@cisco.com

match class-map

To match on the match commands in a specified class map, use the **match class-map** command in the class map configuration mode. To remove the match on the specified class map, use the **no** form of this command.

match [**not**] **class-map** *class-map-name*

no match [**not**] **class-map** *class-map-name*

Syntax Description

not	(Optional) Negates the specified match result.
class-map-name	Matches on the **match** commands in the specified class-map name. The name can be maximum 40 characters.

Command Default

No default behavior or values.

Command Modes

Class-map type qos configuration

Class-map type queuing

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to match on the matches specified in class map named my_test:

```
switch(config)# class-map my_class2
switch(config-cmap-qos)# match class-name my_test
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send feedback to nexus4K-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** configuration, use the **no** form of this command.

match [**not**] **cos** *cos-list*

no match [**not**] **cos** *cos-list*

Syntax Description

not	(Optional) Negates the specified match result.
cos-list	Matches on the specified COS value or list of specified CoS values. Valid values are from 0 to 7.

Command Default

No default behavior or values.

Command Modes

Class map type network qos configuration

Class map type qos configuration

Class map type queuing configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

To specify a list of values, use one of the following options:

- Specify a range of values separated by a dash
- Specify a noncontiguous list of values separated by commas

Any modifications you make to the class map type queuing changes the configuration for all ports of the specified port type on all virtual device contexts (VDC).

Note Only class maps of type qos support the optional **not** keyword form of this command.

This command does not require a license.

Examples

This example shows how to modify a type queuing class map to match on a CoS value:

```
switch(config)# class-map type queuing match-any 1p7q4t-out-q4
switch(config-cmap-que)# match cos 3
switch(config-cmap-que)#
```

This example shows how to remove a match on a CoS value:

```
switch(config)# class-map type queuing match-any 1p7q4t-out-q4
switch(config-cmap-que)# no match cos 3
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config-cmap-que)#
```

Related Commands

Command	Description
show class-map	Displays class maps.

Send feedback to nexus4K-docfeedback@cisco.com

mtu

To configure the interfaces on a switch to transfer large frames on a port, use the **mtu** command. To remove the configured maximum transmission unit (MTU), use the **no** form of this command.

mtu *mtu-value*

no mtu *mtu-value*

Syntax Description

mtu-value	MTU value for the class of service (CoS). Valid values are 1500 to 9216.

Command Default

Default MTU value is 1500. For FCoE cos 3, the default is 2500.

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure MTU for each virtual link in the system.

Examples

This example shows how to set a MTU value for a class in a type network-qos policy map:

```
switch(config)# class-map type network-qos my_class1
switch(config-cmap-nq)# match cos 1-3
switch(config-cmap-nq)# exit
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)# class type network-qos my_class1
switch(config-pmap-nq-c)# mtu 5000
switch(config-pmap-nq-c)#
```

Related Commands

Command	Description
show class-map	Displays class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

pause no-drop

To enable Class Based Flow Control (CBFC) pause characteristics on a class referenced in a type network-qos policy map, use the **pause** command. To disable the CBFC pause characteristics on a class, use the **no** form of this command.

pause no-drop

no pause no-drop

Syntax Description

no-drop	(Optional) Enables no-drop for the CoS on the ingress ports.

Command Default

By default, pause no-drop is on.

Command Modes

Policy map type network-qos class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Ethernet interfaces use priority flow control (PFC) to provide lossless service to no-drop system classes. PFC implements Pause frames on a per-class basis and uses the IEEE 802.1p CoS value to identify the classes that require lossless service.

Examples

This example shows how to enable pause no-drop on a class referenced in a type network-qos policy map:

```
switch(config)# class-map type network-qos my_class1
switch(config-cmap-nq)# match cos 3
switch(config-cmap-nq)# exit
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)# class type network-qos my_class1
switch(config-pmap-nq-c)# pause no-drop
switch(config-pmap-nq-c)#
```

Related Commands

Command	Description
show class-map type network-qos	Displays type network-qos class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

policy-map type network-qos

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

policy-map type network-qos *network-policy-map-name*

no policy-map type network-qos *network-policy-map-name*

Syntax Description

network-policy-map-name	Name assigned to a type network-qos policy map. The name can be maximum 40 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to create or modify a type network-qos policy map:

```
switch(config)# policy-map type network-qos my_policy1
switch(config-pmap-nq)
```

This example shows how to remove a type network-qos policy map:

```
switch(config-pmap-nq)# policy-map type network-qos my_policy1
switch(config)
```

Related Commands

Command	Description
class type network-qos	References a type network-qos class map in a policy map.
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

policy-map type qos

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

policy-map [**type qos**] [**match-first**] *qos-policy-map-name*

no policy-map [**type qos**] [**match-first**] *qos-policy-map-name*

Syntax Description

match-first	(Optional) Specifies that policies associated with the first class that matches the packet characteristics are executed. This is the default action if this option is not specified. **Note** Because this is the default action, you do not need to enter this variable. It is here to ensure compatibility with other systems.
qos-policy-map-name	Name assigned to a type qos policy map. The name can be maximum 40 characters.

Command Default

The software enters the policy map type qos configuration mode if you enter the **policy-map** command without specifying a type.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)#
```

This example shows how to remove a type qos policy map:

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

Related Commands

Command	Description
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

policy-map type queuing

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

policy-map type queuing [**match-first**] *queuing-policy-map-name*

no policy-map type queuing [**match-first**] *queuing-policy-map-name*

Syntax Description

match-first	(Optional) Specifies that policies associated with the first class that matches the packet characteristics are executed. This is the default action if this option is not specified. **Note** Because this is the default action, you do not need to enter this variable; it is here to ensure compatibility with other systems.
queuing-policy-map-name	Name assigned to a type queuing policy map.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

```
switch(config)# policy-map type queuing my_policy1
switch(config-pmap-que)#
```

This example shows how to remove a type queuing policy map:

```
switch(config-pmap-que)# no policy-map type queuing my_policy1
switch(config)#
```

Related Commands

Command	Description
service-policy	Attaches a policy map to an interface.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

priority (queuing)

To configure a single output queuing class as the priority queue, use the **priority** command. To remove the priority queue selection, use the **no** form of this command.

priority [**level** *priority-value*]

no priority [**level** *priority-value*]

Syntax Description

level	(Optional) Specifies the priority level for an output queuing class.
priority-value	Priority level value. Only one priority level is supported. The priority value can only be 1.

Command Default

The software distributes the bandwidth among the output queues, when you do not specify priority.

Command Modes

Policy map type queuing class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The priority level can only be 1.

Use the **bandwidth remaining** command to allocate the remaining bandwidth among the nonpriority output queues. By default, the software evenly distributes the remaining bandwidth among the nonpriority output queues.

Note After you use this command in a specified policy map, you cannot use the **bandwidth** or **shape** command in the same policy map.

This command does not require a license.

Examples

This example shows how to assign a priority queue:

```
switch(config)# policy-map type queuing match-first my_queue
switch(config-pmap-que)# class type queuing 1p3q4t-out-pq1
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)#
```

This example shows how to remove a priority queue:

```
switch(config)# policy-map type queuing match-first my_queue
switch(config-pmap-que)# class type queuing 1p3q4t-out-pq1
switch(config-pmap-c-que)# no priority level 1
switch(config-pmap-c-que)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
bandwidth remaining	Configures the bandwidth remaining on the interface in a queue.
police	Configures policing for specified classes of traffic.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

qos statistics

To enable QoS statistics on all interfaces, use the **qos statistics** command. To disable QoS statistics, use the **no** form of this command.

qos statistics

no qos statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable QoS statistics:

```
switch(config)# qos statistics
switch(config)#
```

This example shows how to disable QoS statistics:

```
switch(config)# no qos statistics
switch(config)#
```

Related Commands

Command	Description
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

service-policy (interface)

To attach a policy map to an interface or tunnel, use the **service-policy** command. To remove a service-policy from an interface or tunnel, use the **no** form of this command.

service-policy {**input** *policy-map-name* | **type** {**qos input** | **queuing output**} *policy-map-name*}

no service-policy {**input** *policy-map-name* | **type** {**qos input** | **queuing output**} *policy-map-name*}

Syntax Description

type	(Optional) Specifies whether the policy map is of type qos or queuing.
qos	Specifies a policy map of type qos.
queuing	Specifies a policy map of type queuing.
input	Applies this policy map to packets coming into this interface.
output	Applies this policy map to packets going out of this interface.
policy-map-name	Name of the policy map to attach to this interface. Only one policy map can be attached to the input and one to the output of a given interface for each of the policy type qos and queuing.

Command Default

Default type is qos.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

No policies of type qos are active on an interface until you enter the **service-policy** command. The system-defined type queuing class maps are attached to each interface unless you specifically attach a different class map. For a list of the system-defined type queuing class maps, see Table 4-1.

You can attach an ingress or egress type policy map to a port, port channel, or tunnel. Only one policy map can be attached to the input and one to the output of a given interface for each of the policy type qos and queuing.

Note For more information on using service policies, see the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide*.

This command does not require a license.

Examples

This example shows how to attach qos type policy maps to the ingress packets of an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# service-policy type qos input my_input_policy
```

Send feedback to nexus4K-docfeedback@cisco.com

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

This example shows how to attach a queuing policy map to the egress packets of a port interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# service-policy type queuing output my_output_policy
switch(config-if)#
```

This example shows how to remove a service policy map from an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no service-policy type queuing output my_output_policy
switch(config-if)#
```

Related Commands

Command	Description
show policy-map interface brief	Displays all interfaces and VLANs with attached service policies in a brief format.
system qos	Configures system policies.

Send feedback to nexus4K-docfeedback@cisco.com

set cos (policy map type qos)

To assign a class of service (CoS) value for a class of traffic in a type qos policy map, use the **set** command. To remove the assigned value from the class, use the **no** form of this command.

set cos *cos-value*

no set cos *cos-value*

Syntax Description

cos-value	Specifies the CoS value to assign for this class of traffic. The range is from 0 to 7.

Command Default

No default behavior or values.

Command Modes

Policy map type qos class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can use this command only on type qos policies that are attached to egress ports.

This command does not require a license.

Examples

This example shows how to assign a CoS value for a class of traffic in a type qos policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)#
```

This example shows how to remove assignment of CoS for a class of traffic in a type qos policy map:

```
switch(config)# policy-map my_policy1
switch(config-pmap-qos)# class traffic_class2
switch(config-pmap-c-qos)# no set cos 3
switch(config-pmap-c-qos)#
```

Related Commands

Command	Description
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

shape

To configure shaping on an egress queue to impose a maximum rate on it, use the **shape** command. To remove a shaping configuration, use the **no** form of this command.

shape {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **average** {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **percent** *percent*}

no shape {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **average** {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **percent** *percent*}

Syntax Description

rate	Specifies the bit rate for shaping an egress queue. Valid values range from 1 to 10000000000.
bps	(Optional) Specifies the units of bits per second.
kbps	(Optional) Specifies the units of kilobits per second.
mbps	(Optional) Specifies the units of megabits per second.
gbps	(Optional) Specifies the units of gigabits per second.
average	(Optional) Specifies an average rate for shaping an egress queue.
percent	Specifies the percentage of the underlying interface link rate. **Note** You can use the **percent** keyword only for interfaces that are set to autonegotiate.
percent-rate	Percent value in the range from 1 to 100.

Command Default

bps is default data rate.

Command Modes

Policy map type queuing class configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You use the system-defined egress queue class for the type of module to which you want to apply the policy map. See Table 4-1 for a list of the system-defined type queuing class maps.

The device forces the shape rate to the closest value in the percentage intervals 100, 50, 25, 12.5, 6.25, 3.13, or 1.07.

Note If you configure shaping, you cannot configure **bandwidth** or **priority** in the same policy map.

This command does not require a license.

Examples

This example shows how to apply shaping based on a percentage rate to a policy map type queuing class:

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config)# policy-map type queuing match-first my_queue
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# shape percent 25
switch(config-pmap-c-que)#
```

This example shows how to apply shaping based on an average rate to a policy map type queuing class:

```
switch(config)# policy-map type queuing match-first my_queue
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# shape 500 mbps
switch(config-pmap-c-que)#
```

This example shows how to remove a shaping configuration from a policy map type queuing class:

```
switch(config)# policy-map type queuing match-first my_queue
switch(config-pmap-que)# class type queuing 1p7q4t-out-pq1
switch(config-pmap-c-que)# no shape percent 25
switch(config-pmap-c-que)#
```

Related Commands

Command	Description
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

show class-map type network-qos

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

show class-map type network-qos [*class-map-name*]

Syntax Description

class-map-name	Name of the class map. The name can be maximum 40 characters.

Command Default

Displays all type network-qos class maps if no class map name is specified.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Table 4-2 displays the list of system-defined class maps that display with this command.

Table 4-2 System-Defined Type network-qos Class Maps

Class Map Name	Description
c-nq-8e	Class map type network-qos in 8-Ethernet.
c-nq-5e-drop	Class map type network-qos in 5-Ethernet. The system drops packets if there is congestion.
c-nq-6e-drop	Class map type network-qos in 6-Ethernet. The system drops packets if there is congestion.
c-nq-5e-ndrop	Class map type network-qos in 5-Ethernet no drop. The system does not drop packets if there is congestion.
c-nq-6e-ndrop	Class map type network-qos in 6-Ethernet no drop. The system does not drop packets if there is congestion.

If you do not specify the type, the command displays all the class maps configured in the system.

This command does not require a license.

Examples

The following is sample output from the **show class-map type network-qos** command and displays all type network-qos class maps:

```
switch(config)# show class-map type network-qos

  Type network-qos class-maps
  ===========================
    class-map type network-qos c-nq-8e
      match cos 0-7
```

Send feedback to nexus4K-docfeedback@cisco.com

```
    class-map type network-qos c-nq-5e-drop
      match cos 0,4-7

    class-map type network-qos c-nq-6e-drop
      match cos 0,2,4-7

    class-map type network-qos c-nq-5e-ndrop
      match cos 1-3

    class-map type network-qos c-nq-6e-ndrop
      match cos 1,3

switch(config)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

show class-map type qos

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

show class-map type qos [*class-map-name*]

Syntax Description		
	class-map-name	Named class map. The name *class-default* is reserved.

Command Default Displays all type qos class maps if no class map name is specified.

Command Modes Any command

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Usage Guidelines When you do not specify the type of class map, the command displays all the class maps configured in the system.

This command does not require a license.

Examples The following is sample output from the **show class-map type qos** command and displays all type qos class maps:

```
switch(config)# show class-map type qos

  Type qos class-maps
  ===================

    class-map type qos match-all cm_qos
      match cos 1,3-5

switch(config)#
```

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

Send feedback to nexus4K-docfeedback@cisco.com

show class-map type queuing

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

show class-map type queuing [*class-map-name*]

Syntax Description

class-map-name	Named class map. The name can be maximum 40 characters.

Command Default

Displays all type queuing class maps if no class map name is specified.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

See Table 4-1 for a list of the system-defined type queuing class maps.

This command does not require a license.

Examples

The following is sample output from the **show class-map type queuing** command and displays all type queuing class maps:

```
switch(config)# show class-map type queuing

  Type queuing class-maps
  ========================

    class-map type queuing match-any 1p7q4t-out-pq1
      Description: Classifier for egress priority queue of type 1p7q4t
      match cos 1

    class-map type queuing match-any 1p7q4t-out-q2
      Description: Classifier for egress queue 2 of type 1p7q4t
      match cos 2

    class-map type queuing match-any 1p7q4t-out-q3
      Description: Classifier for egress queue 3 of type 1p7q4t
      match cos 0

    class-map type queuing match-any 1p7q4t-out-q4
      Description: Classifier for egress queue 4 of type 1p7q4t
      match cos 4

    class-map type queuing match-any 1p7q4t-out-q5
      Description: Classifier for egress queue 5 of type 1p7q4t
      match cos 5

    class-map type queuing match-any 1p7q4t-out-q6
      Description: Classifier for egress queue 6 of type 1p7q4t
```

Send feedback to nexus4K-docfeedback@cisco.com

```
      match cos 6

    class-map type queuing match-any 1p7q4t-out-q7
      Description: Classifier for egress queue 7 of type 1p7q4t
      match cos 7

    class-map type queuing match-any 1p7q4t-out-q-default
      Description: Classifier for egress default queue of type 1p7q4t
      match cos 3

switch(config)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

show policy-map

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

show policy-map [**type** {**network-qos** | **qos** | **queuing**} *policy-map-name*]

Syntax Description

type	(Optional) Specifies the component type to display.
network-qos	Displays policy maps of type network-qos.
qos	Displays policy maps of type qos.
queuing	Displays policy maps of type queuing.
policy-map-name	(Optional) Name of a policy map.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify a policy map type and name, the system displays all the policy maps.

Examples

The following is sample output from the **show policy-map** command and displays information about a specific policy map:

```
switch(config)# show policy-map my_policy1

Type qos policy-maps
  ====================

  policy-map type qos my_policy1
    class  abc
      set cos 3
switch(config)#
```

The following is sample output from the **show policy-map type queuing** command and displays all type queuing policy maps:

```
switch(config)# show policy-map type queuing

  Type queuing policy-maps
  ========================

  policy-map type queuing default-out-policy
    class type queuing 1p7q4t-out-q3
      bandwidth percent 12
    class type queuing 1p7q4t-out-pq1
```

Send feedback to nexus4K-docfeedback@cisco.com

```
      bandwidth percent 12
    class type queuing 1p7q4t-out-q2
      bandwidth percent 12
    class type queuing 1p7q4t-out-q-default
      bandwidth percent 12
    class type queuing 1p7q4t-out-q4
      bandwidth percent 12
    class type queuing 1p7q4t-out-q5
      bandwidth percent 12
    class type queuing 1p7q4t-out-q6
      bandwidth percent 12
    class type queuing 1p7q4t-out-q7
      bandwidth percent 12
  policy-map type queuing policy-fcoe-bandwidth
    class type queuing 1p7q4t-out-q-default
      bandwidth percent 50
    class type queuing 1p7q4t-out-pq1
      bandwidth percent 7
switch(config)#
```

The following is sample output from the **show policy-map type network-qos** command and displays all type network-qos policy maps:

```
switch(config)# show policy-map type network-qos

  Type network-qos policy-maps
  ============================

    policy-map type network-qos pm_nq
        class-map  cm_nq
        pause no-drop

    policy-map type network-qos p-nq-5e
        class-map  c-nq-5e-drop
        class-map  c-nq-5e-ndrop
        pause no-drop
        mtu 2240

    policy-map type network-qos p-nq-6e
        class-map  c-nq-6e-drop
        class-map  c-nq-6e-ndrop
        pause no-drop
        mtu 2240

    policy-map type network-qos p-nq-8e
        class-map  c-nq-8e

    policy-map type network-qos policy-fcoe
        class-map  class-fcoe
        pause no-drop
        mtu 2500
        class-map  class-non-fcoe

switch(config)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

show policy-map interface

To display policy maps and statistics for the interfaces, use the **show policy-map interface** command.

show policy-map interface [**ethernet** {*slot/port*} | **input** | **output** | **port-channel** {*channel-number***}** | **type** {**qos** | **queuing**}]

Syntax Description

ethernet	(Optional) Displays policy maps assigned to Ethernet interfaces.
slot/port	Ethernet interface slot and port number. The range is from 1 to 1.
input	(Optional) Displays policy maps assigned to input traffic.
output	(Optional) Displays policy maps assigned to output traffic.
port-channel	(Optional) Displays policy maps assigned to port channels.
channel-number	Port channel number. Valid values are 1 to 576.
type	(Optional) Specifies the component type to display.
qos	Displays policy maps of type qos.
queuing	Displays policy maps of type queuing.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Statistics are on by default.

This command does not require a license.

Examples

The following is sample output from the **show policy-map interface ethernet** command and displays policy maps assigned to a specified interface:

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


Global statistics status :   enabled

Ethernet1/1

  Service-policy (queuing) output:   policy-fcoe-bandwidth
    policy statistics status:   disabled

    Class-map (queuing):   1p7q4t-out-q-default (match-any)
      bandwidth percent 50
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config)#
```

Related Commands

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

Send feedback to nexus4K-docfeedback@cisco.com

show policy-map interface brief

To display a brief report of all policy maps applied to interfaces, use the **show policy-map interface brief** command.

show policy-map interface brief

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following is sample output from the **show policy-map interface brief** command and displays a brief information about the policy maps assigned to interfaces:

```
switch(config)# show policy-map interface brief

 Interface      [Status]:INP QOS        OUT QUE
================================================
Ethernet1/1     [Active]:              policy-fcoe-b
Ethernet1/2     [Active]:              policy-fcoe-b
Ethernet1/3     [Active]:              policy-fcoe-b
Ethernet1/4     [Active]:              policy-fcoe-b
Ethernet1/5     [Active]:              policy-fcoe-b
Ethernet1/6     [Active]:              policy-fcoe-b
Ethernet1/7     [Active]:              policy-fcoe-b
Ethernet1/8     [Active]:              policy-fcoe-b
Ethernet1/9     [Active]:              policy-fcoe-b
Ethernet1/10    [Active]:              policy-fcoe-b
Ethernet1/11    [Active]:              policy-fcoe-b
Ethernet1/12    [Active]:              policy-fcoe-b
Ethernet1/13    [Active]:              policy-fcoe-b
Ethernet1/14    [Active]:              policy-fcoe-b
Ethernet1/15    [Active]:              policy-fcoe-b
Ethernet1/16    [Active]:              policy-fcoe-b
Ethernet1/17    [Active]:              policy-fcoe-b
Ethernet1/18    [Active]:              policy-fcoe-b
Ethernet1/19    [Active]:              policy-fcoe-b
Ethernet1/20    [Active]:              policy-fcoe-b
================================================
switch(config)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

show queuing interface

To display queuing information on a specified interface, use the **show queuing interface** command.

show queuing interface ethernet *slot/port*

Syntax Description

slot/port	Ethernet interface slot and port number. The range is from 1 to 1.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following is sample output from the **show queuing interface ethernet** command and displays the queuing information for a specified interface:

```
switch# show queuing interface ethernet 1/1
Queuing Configs for interface 0x1a000000(System)
Port QOS is enabled
Transmit queues [type = 1p7q4t]
Queue ID                                COS     Scheduling
-----------------------------------------------------------

1p7q4t-out-q3                            0       WRR
1p7q4t-out-pq1                           1       WRR
1p7q4t-out-q2                            2       WRR
1p7q4t-out-q-default                     3       WRR
1p7q4t-out-q4                            4       WRR
1p7q4t-out-q5                            5       WRR
1p7q4t-out-q6                            6       WRR
1p7q4t-out-q7                            7       WRR

Queue ID                                B/W     Shape
-----------------------------------------------------------

1p7q4t-out-q-default        BW percent Gua:50, Rem:0, RemReal:0
       -
1p7q4t-out-pq1              BW percent Gua:7, Rem:0, RemReal:0
       -
1p7q4t-out-q2               BW percent Gua:7, Rem:0, RemReal:0
       -
1p7q4t-out-q3               BW percent Gua:7, Rem:0, RemReal:0
       -
1p7q4t-out-q4               BW percent Gua:7, Rem:0, RemReal:0
       -
```

Send feedback to nexus4K-docfeedback@cisco.com

```
1p7q4t-out-q5               BW percent Gua:7, Rem:0, RemReal:0
       -
1p7q4t-out-q6               BW percent Gua:7, Rem:0, RemReal:0
       -
1p7q4t-out-q7               BW percent Gua:7, Rem:0, RemReal:0
       -

------------------------------------------------------
Queuing configs for 1p7q4t-out-q-default**
Group-id: 0
Flags: 0x1
BW percent Gua:50, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-pq1**
Group-id: 1
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-q2**
Group-id: 2
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-q3**
Group-id: 3
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-q4**
Group-id: 4
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-q5**
Group-id: 5
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-q6**
Group-id: 6
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0
Queuing configs for 1p7q4t-out-q7**
Group-id: 7
Flags: 0x1
BW percent Gua:7, Rem:0, RemReal:0

switch#
```

Related Commands

Command	Description
show class-map type queuing	Displays information about type queuing class maps.
show policy-map	Displays policy maps and statistics.

Send feedback to nexus4K-docfeedback@cisco.com

show running-config ipqos

To display information about the running-system configuration for Quality of Service (QoS), use the **show running-config ipqos** command.

show running-config ipqos [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

No default behavior or values.

Command Modes

Any command

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following is sample output from the **show running-config ipqos** command and displays information about QoS:

```
switch(config)# show running-config ipqos

version 4.1(2)E1(1)
system jumbomtu 9214
class-map type qos match-all cm_qos
  match cos 1,3-5
policy-map type qos pm-qos
policy-map type qos pm_qos
  class cm_qos
policy-map type queuing pm_nq
  class type queuing 1p7q4t-out-q2
policy-map type queuing policy-fcoe-bandwidth
  class type queuing 1p7q4t-out-q-default
    bandwidth percent 50
class-map type network-qos cm_nq
  match cos 5
class-map type network-qos class-fcoe
  match cos 3
class-map type network-qos class-non-fcoe
  match cos 0-2,4-7
policy-map type network-qos pm_nq
  class type network-qos cm_nq
    pause no-drop
policy-map type network-qos policy-fcoe
  class type network-qos class-fcoe
    pause no-drop
    mtu 7000
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  class type network-qos class-non-fcoe
policy-map type network-qos policy-non-fcoe
  class type network-qos class-non-fcoe
    mtu 7000
system qos
  service-policy type queuing output default-out-policy

switch(config)#
```

Related Commands

Command	Description
show class-map	Displays information about class maps.
show policy-map	Displays statistics and information about policy maps.

Send feedback to nexus4K-docfeedback@cisco.com

system jumbomtu

To define the maximum transmission units (MTU) of packets in the system, use the **system jumbomtu** command. To revert to the default MTU setting, use the **no** form of this command.

system jumbomtu *mtu-size*

no system jumbomtu

Syntax Description

mtu-size	Maximum size of packets. Valid values are from 2240 to 9216.

Command Default

9216 bytes

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When you set the global system MTU size, the packets that are larger than the system MTU size are not transmitted on the egress.

Examples

This example shows how to set the global MTU size to 5000 bytes:

```
switch(config)# system jumbomtu 5000
```

This example shows how to revert to the default MTU setting:

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

Related Commands

Command	Description
mtu	Configures the maximum packet size or MTU size for interfaces.
show interface	Displays the jumbo MTU frames sent and received on the specified interface.

Send feedback to nexus4K-docfeedback@cisco.com

system qos

To configure system policy, use the **system qos** command.

system qos

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to configure a system qos to apply a queuing policy to all interfaces in the system:

```
switch# configure terminal
switch(config)# system qos
switch(config-sys-qos)# service-policy type queueing output my_policy1
```

Related Commands

Command	Description
service- policy	Associates the system class policy-map to the service policy for the system.

Send feedback to nexus4K-docfeedback@cisco.com



CHAPTER 5

Security Commands

This chapter describes the Cisco NX-OS security commands available on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

aaa accounting default

To configure the authentication, authorization, and accounting (AAA) accounting feature to use the default accounting method for accounting services, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

aaa accounting default {**group** *server-group-list* | **local**}

no aaa accounting default {**group** *server-group-list* | **local**}

Syntax Description

group	Specifies that a server group be used for the accounting services.
server-group-list	Specifies a space-delimited 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 The server group list can be maximum 127 characters.
local	Specifies that the local database be used for accounting.

Command Default

The local database is the default.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The AAA accounting feature tracks the services that users are accessing and the network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server, or the local database, in the form of accounting records.

The **group** *server-group-list* method refers to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method, or the **local** method, or both and they fail, the accounting authentication fails.

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch(config)# aaa accounting default group radius
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
aaa group server tacacs+	Configures TACACS+ server groups.
radius-server host	Specifies a RADIUS server host.
show aaa accounting	Displays AAA accounting status information.
show startup-config aaa	Displays the AAA configuration in the startup configuration.
tacacs-server host	Specifies a TACACS+ server host.

Send feedback to nexus4K-docfeedback@cisco.com

aaa authentication login console

To configure AAA authentication methods for console logins, use the **aaa authentication login console** command. To disable AAA authentication, 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 that a server group be used for authentication.
group-list	Specifies a space-delimited 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 there is no authentication to get to the console access.
local	(Optional) Specifies that console access is authenticated by a local username and password.

Command Default

The local database.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 **local** method, a username and password have to be configured in the local database of the switch. Local is the default and is used when no authentication methods are configured or when all the configured methods fail to respond.

If you specify the **group** method or **local** method and they fail, the authentication can fail. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

Examples

This example shows how to have console access authenticated using a server group:

```
switch(config)# aaa authentication login console group radius
```

Send feedback to nexus4K-docfeedback@cisco.com

This example shows how to have console access authenticated by a local username and password:

```
switch(config)# aaa authentication login console local
```

This example shows how to have no authentication:

```
switch(config)# aaa authentication login console none
```

This example shows how to disable console access authentication using a server group:

```
switch(config)# no aaa authentication login console group radius
```

Related Commands

Command	Description
aaa group server radius	Configures RADIUS server groups.
aaa group server tacacs+	Configures TACACS+ server groups.
radius-server host	Specifies a RADIUS server host.
show aaa authentication	Displays AAA authentication information.
show aaa groups	Displays the AAA server groups.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.
tacacs-server host	Specifies a TACACS+ server host.

Send feedback to nexus4K-docfeedback@cisco.com

aaa authentication login default

To configure the default AAA authentication methods, use the **aaa authentication login default** command. To disable AAA authentication, 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 there is no authentication.
local	(Optional) Specifies that authentication is done using a local username and password.

Command Default

The local database.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 **local** method, a username and password have to be configured in the local database of the switch. Local is the default and is used when no authentication methods are configured or when all the configured methods fail to respond.

If you specify the **group** method or **local** method and they fail, the authentication fails. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

Examples

This example shows how to configure default AAA authentication using a server group:

```
switch(config)# aaa authentication login default group radius
```

This example shows how to disable the default AAA authentication using a server group:

```
switch(config)# no aaa authentication login default group radius
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
aaa group server tacacs+	Configures AAA TACACS+ server groups.
radius-server host	Specifies a RADIUS server host.
show aaa authentication	Displays AAA authentication information.
show aaa groups	Displays the AAA server groups.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.
tacacs-server host	Specifies a TACACS+ server host.

Send feedback to nexus4K-docfeedback@cisco.com

aaa authentication login error-enable

To configure a AAA authentication failure message to display on the console, use the **aaa authentication login error-enable** command. To disable the display of AAA authentication failure messages on the console, use the **no** form of this command.

aaa authentication login error-enable

no aaa authentication login error-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If none of the remote AAA servers respond when a user logs in, the authentication is processed by the local user database. If you have enabled the display, one of the following message is generated for the user:

```
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.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

Send feedback to nexus4K-docfeedback@cisco.com

aaa authentication login mschap enable

To enable Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication at login, use the **aaa authentication login mschap enable** command. To disable MS-CHAP, 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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable MS-CHAP authentication:

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

This example shows how to disable MS-CHAP authentication:

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

Related Commands

Command	Description
show aaa authentication	Displays the status of MS-CHAP authentication.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

Send feedback to nexus4K-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 remove a RADIUS server group from the configuration list, use the **no** form of this command.

aaa group server radius *server-group-name*

no aaa group server radius *server-group-name*

Syntax Description

server-group-name	RADIUS server group name. The name is alphanumeric and case-sensitive. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to create a RADIUS server group and enter RADIUS server configuration mode:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
switch(config-radius)# no aaa group server radius RadServer
```

Related Commands

Command	Description
radius server host	Defines the IP address or hostname for a RADIUS server.
show aaa groups	Displays AAA server group information.
show radius-server	Displays RADIUS server information.

Send feedback to nexus4K-docfeedback@cisco.com

aaa group server tacacs+

To create a Terminal Access Controller Access Control System Plus (TACACS+) server group and enter TACACS+ server group configuration mode, use the **aaa group server tacacs+** command. To delete a TACACS+ server group, use the **no** form of this command.

aaa group server tacacs+ *server-group-name*

no aaa group server tacacs+ *server-group-name*

Syntax Description

server-group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you can configure TACACS+ server groups, you must enable TACACS+ on the switch by using the **feature tacacs+** command. The commands for configuring TACACS+ server groups are not visible until you enable TACACS+.

Examples

This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:

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

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

```
switch(config-tacacs+)# no aaa group server tacacs+ TacServer
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show aaa groups	Displays AAA server group information.
show tacacs-server	Displays TACACS+ server information.
tacacs+ hostname	Defines the IP address or hostname for a TACACS+ server.

Send feedback to nexus4K-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** | **redirect ethernet** *slot*}

no action {**drop** | **forward** | **redirect ethernet** *slot*}

Syntax Description

drop	Specifies that the switch drops the packet.
forward	Specifies that the switch forwards the packet to its destination port.
redirect	Specifies that the switch redirect the packets to a specified interface.
ethernet	Specifies the Ethernet interface the packet should be forwarded to.
slot	Ethernet interface slot number and port number specified in the format 1/1.

Command Default

No default behavior or values.

Command Modes

Vlan access-map configuration

Command History

Release	Modification
4.1(2)E1(1)	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, and specifies that the switch forwards packets matching the ACL:

```
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)#
```

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.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send feedback to nexus4K-docfeedback@cisco.com

clear access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv4 ACL whose counters the switch clears. The name cannot contain a space, and can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear counters for all IPv4 ACLs:

```
switch# clear access-list counters
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
```

Related Commands

Command	Description
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, and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear the accounting log:

```
switch# clear accounting log
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

Send feedback to nexus4K-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

Radius server group configuration

Tacacs+ server group configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 feedback to nexus4K-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**]

no deny *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [*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**]

Send feedback to nexus4K-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 a protocol. The *protocol* argument can be one of the keywords **icmp**, **igmp**, **ip**, **tcp**, or **udp**, or an integer in the range from 0 to 255. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**.
icmp	Specifies that the rule applies only to ICMP traffic.
igmp	Specifies that the rule applies only to Internet Group Management Protocol (IGMP) traffic.
ip	Specifies that the rule applies to all IP traffic.
tcp	Specifies that the rule applies only to TCP traffic.
udp	Specifies that the rule applies only to UDP traffic.
source	Specifies the 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	Specifies the 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.
dscp *dscp*	(Optional) Matches the packets with the given 6-bit Differentiated Services Code Point (DSCP) value. See “DSCP Values” in the “Usage Guidelines” section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets. See “Precedence Values” in the “Usage Guidelines” section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets. The fragment is either permitted or denied accordingly. **Note** 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.
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.

Send feedback to nexus4K-docfeedback@cisco.com

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
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 can be **eq** (Equal), **gt** (Greater Than), **lt** (Less Than), **neq** (Note Equal To), or **range** (range of port numbers).
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies the source or destination IP port object group name. 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. **Note** 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**—Acknowledge the successful receipt of packets. • **fin**—(Finish) Close the TCP session. • **psh**—(Push) Forcefully deliver data without waiting for buffers to fill. • **rst**—Reset the connection to the remote host. • **syn**—Synchronize sequence numbers during TCP connections. • **urg**—Incoming packets marked as "urgent" are processed immediately.
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 feedback to nexus4K-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
4.1(2)E1(1)	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. The syntax is as follows:

  addrgroup *address-group-name*

  Note Use the **object-group ip address** command to create and change IPv4 address group objects.

- 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

- 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

- 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.

- 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.

DSCP Values

The *dscp* argument can be a number, which is an integer from 0 to 63 that is 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.

Send feedback to nexus4K-docfeedback@cisco.com

The *dscp* argument can also be a keyword. Table 5-1 lists the DSCP values.

Table 5-1 DSCP Values

DSCP Value	Description
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)

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also a keyword. Table 5-2 lists the ICMP message types.

Table 5-2 ICMP Message Types

ICMP Message	Description
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

Send feedback to nexus4K-docfeedback@cisco.com

Table 5-2 ICMP Message Types (continued)

ICMP Message	Description
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachable	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for ToS
host-tos-unreachable	Host unreachable for ToS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Net redirect for ToS
net-tos-unreachable	Network unreachable for ToS
net-unreachable	Net unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present
packet-too-big	Fragmentation needed and DF set
parameter-problem	All parameter problems
port-unreachable	Port unreachable
precedence-unreachable	Precedence cutoff
protocol-unreachable	Protocol unreachable
reassembly-timeout	Reassembly timeout
redirect	All redirects
router-advertisement	Router discovery advertisements
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

Send feedback to nexus4K-docfeedback@cisco.com

Table 5-2 ICMP Message Types (continued)

ICMP Message	Description
ttl-exceeded	TTL exceeded
unreachable	All unreachables

Precedence Values

The *precedence* argument can be a number or a keyword. Table 5-3 lists the precedence keywords.

Table 5-3 Precedence Value

Precedence Value	Description
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)

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 a keyword. Table 5-4 lists the TCP port names.

Table 5-4 TCP Ports

TCP Port	Description
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)

Send feedback to nexus4K-docfeedback@cisco.com

Table 5-4 TCP Ports (continued)

TCP Port	Description
gopher	Gopher (7)
hostname	NIC hostname server (11)
ident	Ident Protocol (113)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
login	Login (rlogin, 513)
lpd	Printer service (515)
nntp	Network News Transport Protocol (119)
pim-auto-rp	PIM Auto-RP (496)
pop2	Post Office Protocol v2 (19)
pop3	Post Office Protocol v3 (11)
smtp	Simple Mail Transport Protocol (25)
sunrpc	Sun Remote Procedure Call (111)
tacacs	TAC Access Control System (49)
talk	Talk (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (54)
whois	WHOIS/NICNAME (43)
www	World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be a keyword. Table 5-5 lists the UDP ports.

Table 5-5 UDP Ports

UDP Port	Description
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 System (DNS, 53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (5)
mobile-ip	Mobile IP registration (434)

Send feedback to nexus4K-docfeedback@cisco.com

Table 5-5 UDP Ports (continued)

UDP Port	Description
nameserver	IEN116 name service (obsolete, 42)
netbios-dgm	NetBIOS datagram service (138)
netbios-ns	NetBIOS name service (137)
netbios-ss	NetBIOS session service (139)
non500-isakmp	Internet Security Association and Key Management Protocol (45)
ntp	Network Time Protocol (123)
pim-auto-rp	PIM Auto-RP (496)
rip	Routing Information Protocol (router, in.routed, 52)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs	TAC Access Control System (49)
talk	Talk (517)
tftp	Trivial File Transfer Protocol (69)
time	Time (37)
who	Who service (rwho, 513)
xdmcp	X Display Manager Control Protocol (177)

Examples

This 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
```

This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.2.0 subnet:

```
switch(config-acl)# deny tcp 192.168.2.0 192.168.2.255 any
```

This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.2.0 subnet:

```
switch(config-acl)# deny udp 192.168.2.0/24 any
```

This example shows how to specify the *source* argument with the **host** keyword and the 192.168.2.132 IPv4 address:

```
switch(config-acl)# deny icmp host 192.168.2.132 any
```

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 192.168.2.23 and 192.168.2.37 networks to the 192.168.0.0 network and a final rule that permits all other IPv4 traffic:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 192.168.2.23/16 192.168.0.0/16
switch(config-acl)# deny udp 192.168.2.23/16 192.168.0.0/16
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config-acl)# deny tcp 192.168.2.37/16 192.168.0.0/16
switch(config-acl)# deny udp 192.168.2.37/16 192.168.0.0/16
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.
object-group ip address	Configures an IPv4 address group object.
object-group ip port	Configures an IPv4 port group object.
remark	Configures a remark in an IPv4 or MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.

Send feedback to nexus4K-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*]

no deny *source destination* [*protocol*] [**cos** *cos-value*]

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. Use the format EEEE.EEEE.EEEE. 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. Use the format EEEE.EEEE.EEEE. 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.

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 feedback to nexus4K-docfeedback@cisco.com

Command History

Release	Modification
4.1(2)E1(1)	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 example 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 feedback to nexus4K-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)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
mac access-list	Configures a MAC ACL.
permit (MAC)	Configures a deny rule in a MAC ACL.
remark	Configures a remark in an IPv4 or MAC ACL.
show mac access-lists	Displays all MAC ACLs or one MAC ACL.

Send feedback to nexus4K-docfeedback@cisco.com

description (user role)

To add 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 string can be maximum 128 characters.

Command Default

No default behavior or values.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can include blank spaces in the user role description text.

Examples

This example shows how to configure the description for a user role:

```
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

This example shows how to remove the description from a user role:

```
switch(config)# role name MyRole
switch(config-role)# no description
```

Related Commands

Command	Description
show role	Displays the user role configuration.

Send feedback to nexus4K-docfeedback@cisco.com

feature (role feature-group)

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. The name has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

No default behavior or values.

Command Modes

User role feature group configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the **show role feature** command to list the valid feature names to use in this command.

Examples

This example shows how to add features to a user role feature group:

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

This example shows how to remove a feature from a user role feature group:

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# no feature tacacs
```

Related Commands

Command	Description
role feature-group name	Creates or configures a user role feature group.
show role feature	Displays the user role features.
show role feature-group	Displays the user role feature groups.

Send feedback to nexus4K-docfeedback@cisco.com

interface policy deny

To configure the interface policy for a user role, and enter interface policy configuration mode for the 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
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter interface policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

This example shows how to revert to the default interface policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

Related Commands

Command	Description
permit interface	Permits access to interfaces for a user role interface policy.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send feedback to nexus4K-docfeedback@cisco.com

ip access-list

To define an IPv4 access control list (ACL) and add rules to it 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. The name can be up to 64 characters long, and cannot contain a space or quotation mark.

Command Default

No IPv4 ACL is defined.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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) 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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
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 feedback to nexus4K-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

No IPv4 ACLs are applied to an interface.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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

- Layer 2 Ethernet interfaces
- Layer 2 EtherChannel interfaces

You can also apply an IPv4 ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

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

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group ip-acl-01 in
switch(config-if)# show running-config interface ethernet 1/2
version 4.1(2)E1(1)

interface Ethernet1/2
  ip port access-group ip-acl-01 in
switch(config-if)#
```

Send feedback to nexus4K-docfeedback@cisco.com

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
copy running-config startup-config	Copies the running configuration to the startup configuration.
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 feedback to nexus4K-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. The name cannot contain a space or quotation mark, and must be maximum 64 characters.

Command Default

No MAC ACLs are defined by default.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use MAC ACLs to filter non-IP traffic. If you disable packet classification, you can use MAC ACLs to filter all 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 port 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-mac-acl)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac port access-group	Applies a MAC ACL to an interface.
permit (MAC)	Configures a permit rule in a MAC ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

Send feedback to nexus4K-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. The name is case-sensitive, and can be up to 64 alphanumeric characters.

Command Default

No MAC ACLs are applied to an interface.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

MAC ACLs apply to non-IP traffic. If packet classification is disabled, MAC ACLs apply to all traffic.

You can use the **mac port access-group** command to apply a MAC ACL as a port ACL to the following interface types:

- Layer 2 interfaces
- Layer 2 EtherChannel interfaces

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

The switch applies MAC ACLs only to inbound traffic. When the switch applies a MAC ACL, the switch checks packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply a MAC ACL named mac-acl-01 to Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
```

This example shows how to remove a MAC ACL named mac-acl-01 from Ethernet interface 1/2:

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

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
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 feedback to nexus4K-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** | **mac**} **address** *access-list-name*

no match {**ip** | **mac**} **address** *access-list-name*

Syntax Description

ip	The specified ACL is an IPv4 ACL.
mac	The specified ACL is a MAC ACL.
address *access-list-name*	Specifies the ACL name. The name is case-sensitive and can be maximum 64 characters.

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
4.1(2)E1(1)	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, and assigns an IPv4 ACL named ip-acl-01 to the map:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)#
```

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.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

Send feedback to nexus4K-docfeedback@cisco.com

object-group ip address

To create and change IPv4 address group objects, use the **object-group ip address** command. To remove an address group, use the **no** form of this command.

object-group ip address *obj-group-name*

no object-group ip address *obj-group-name*

Syntax Description

obj-group-name	Name of the IP address group object. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use this command to create IP address groups that you can use as the source or destination address in an IPv4 ACL configuration.

Examples

This example shows how to create an IP address group:

```
switch(config)# object-group ip address lab-gateway-svrs
switch(config)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.

Send feedback to nexus4K-docfeedback@cisco.com

object-group ip port

To create and change IPv4 port-group objects, use the **object-group ip address** command. To remove a port-group object, use the **no** form of this command.

object-group ip port *obj-group-name*

no object-group ip port *obj-group-name*

Syntax Description

obj-group-name	Name of the port-group object. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use this command to create IP port-groups that you can use as the source or destination port-group in an IPv4 ACL configuration.

Examples

This example shows how to create an port group object:

```
switch(config)# object-group ip port lab-gateway-port
switch(config)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.

Send feedback to nexus4K-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**]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Group Management Protocol

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Protocol v4

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Transmission Control Protocol

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [*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**]

Send feedback to nexus4K-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. The *protocol* argument can be one of the keywords **icmp**, **igmp**, **ip**, **tcp**, or **udp**, or an integer in the range from 0 to 255. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**.
icmp	Specifies that the rule applies only to ICMP traffic.
igmp	Specifies that the rule applies only to Internet Group Management Protocol (IGMP) traffic.
ip	Specifies that the rule applies to all IPv4 traffic.
tcp	Specifies that the rule applies only to TCP traffic. Table 5-4 lists the TCP ports.
udp	Specifies that the rule applies only to UDP traffic. Table 5-5 lists the UDP ports.
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.
dscp *dscp*	(Optional) Matches the packets with the given 6-bit Differentiated Services Code Point (DSCP) value. Table 5-1 lists the DSCP values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets. Table 5-3 lists the precedence values that you can use to define the ACL.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets. The fragment is either permitted or denied accordingly. **Note** 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.
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 in Table 5-2.

Send feedback to nexus4K-docfeedback@cisco.com

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
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 can be **eq** (Equal), **gt** (Greater Than), **lt** (Less Than), **neq** (Note Equal To), or **range** (range of port numbers).
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies the source or destination IP port object group name. 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. **Note** 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**—Acknowledge the successful receipt of packets. • **fin**—(Finish) Close the TCP session. • **psh**—(Push) Forcefully deliver data without waiting for buffers to fill. • **rst**—Reset the connection to the remote host. • **syn**—Synchronize sequence numbers during TCP connections. • **urg**—Incoming packets marked as “urgent” are processed immediately.
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 feedback to nexus4K-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
4.1(2)E1(1)	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. The syntax is as follows:

  addrgroup *address-group-name*

  Note Use the **object-group ip address** command to create and change IPv4 address group objects.

- 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

- 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

- 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.

- 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.

Examples

This 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
```

Send feedback to nexus4K-docfeedback@cisco.com

This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.2.0 subnet:

```
switch(config-acl)# permit tcp 192.168.2.0 192.0.2.255 any
```

This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.2.0 subnet:

```
switch(config-acl)# permit udp 192.168.2.0/24 any
```

This example shows how to specify the *source* argument with the **host** keyword and the 192.168.2.132 IPv4 address:

```
switch(config-acl)# permit icmp host 192.168.2.132 any
```

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 192.168.2.23 and 192.168.2.37 networks to the 192.168.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 192.168.2.23/16 192.168.0.0/16
switch(config-acl)# permit udp 192.168.2.23/16 192.168.0.0/16
switch(config-acl)# permit tcp 192.168.2.37/16 192.168.0.0/16
switch(config-acl)# permit udp 192.168.2.37/16 192.168.0.0/16
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-list	Configures an IPv4 ACL.
object-group ip address	Configures an IPv4 address group object.
object-group ip port	Configures an IPv4 port group object.
remark	Configures a remark in an IPv4 or MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.

Send feedback to nexus4K-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. Use the format EEEE.EEEE.EEEE. 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. Use the format EEEE.EEEE.EEEE. 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 feedback to nexus4K-docfeedback@cisco.com

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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 IPv4 or MAC ACL.
show mac access-lists	Displays all MAC ACLs or one MAC ACL.

Send feedback to nexus4K-docfeedback@cisco.com

permit interface

To allow access to interfaces for a user role interface policy, use the **permit interface** command. To remove the allowed interfaces, use the **no** form of this command.

permit interface {**ethernet** *slot* | **port-channel** *number*}

no permit interface {**ethernet** *slot* | **port-channel** *number*}

Syntax Description

ethernet *slot*	Specifies the Ethernet interface slot number and port number in the format 1/1.
port-channel *number*	Specifies the EtherChannel number. Valid EtherChannel numbers are from 1 to 576.

Command Default

All interfaces.

Command Modes

Interface policy configuration

Command History

Release	Modification
4.1(2)E1(1)	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 an allowed 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
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
interface policy deny	Enters interface 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 feedback to nexus4K-docfeedback@cisco.com

permit vlan

To specify the range of VLANs that the role can access, use the **permit vlan** command. To remove VLAN access, 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
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
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 feedback to nexus4K-docfeedback@cisco.com

permit vrf

To specify the range of Virtual Private Network (VPN) routing and forwarding (VRF) instances the role can access, 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. The default VRFs include the following: • **chassis-management** • **default** • **management**

Command Default

All VRFs.

Command Modes

Vrf policy configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the **show vrf** command to display a list of VRFs in the system. You can also create VRFs using the **vrf context** command.

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
switch(config-role-vrf)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
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 feedback to nexus4K-docfeedback@cisco.com

Command	Description
show vrf	Displays the list of VRFs.
vrf context	Creates a VRF instance.

Send feedback to nexus4K-docfeedback@cisco.com

radius-server deadtime

To configure the global dead-time interval for all RADIUS servers on a switch, use the **radius-server deadtime** command. To restore the default dead-time interval of 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Command Default

0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 specify five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

```
switch(config)# radius-server deadtime 5
```

This example shows how to revert to the default 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 feedback to nexus4K-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 disable the directed-request feature, 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

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

The **no radius-server directed-request** command causes the entire username string, both before and after the "@" symbol, to be passed to the default RADIUS server.

Examples

This example shows how to enable directed requests to a specific RADIUS server:

```
switch(config)# radius-server directed-request
```

This example shows how to disable directed requests to a specific RADIUS server:

```
switch(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server	Displays the directed request configuration in a RADIUS server.

Send feedback to nexus4K-docfeedback@cisco.com

radius-server host

To define a RADIUS server host to be used for authentication, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address*}
[**accounting [retransmit** *count* | **timeout** *seconds*]]
[**acct-port** *port-number*]
[**auth-port** *port-number*]
[**authentication** [**accounting** [**transmit** | **timeout** *seconds*]]]
[**key** {**0** | **7** | *key-value*}]
[**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address*}
[**accounting [retransmit** *count* | **timeout** *seconds*]]
[**acct-port** *port-number*]
[**auth-port** *port-number*]
[**authentication** [**accounting** [**transmit** | **timeout** *seconds*]]]
[**key** {**0** | **7** | *key-value*}]
[**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name System (DNS) name. The maximum length is 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
key	(Optional) Configures a preshared key for a single RADIUS server host. This preshared key is used instead of the global preshared 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.
key-value	Configures a preshared key to authenticate communication between the RADIUS client and server. The maximum length is 63 characters.
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.

Send feedback to nexus4K-docfeedback@cisco.com

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.
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

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 specify host1 as the RADIUS server and use the default ports for both accounting and authentication:

```
switch(config)# radius-server host host1
```

This example shows how to specify port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
switch(config)# radius-server host host1 auth-port 1612 acct-port 1616
```

This example shows how to configure the host with IP address 192.168.2.1 as the RADIUS server, ports 2003 and 2004 as the authorization and accounting ports, enable accounting services on the RADIUS server, set the clear text and encrypted shared keys, set the idle time value to 10 minutes, and set the username and password for test packets on the RADIUS server:

```
switch(config)# radius-server host 192.168.2.1 key HostKey
switch(config)# radius-server host 192.168.2.1 auth-port 2003
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config)# radius-server host 192.168.2.1 acct-port 2004
switch(config)# radius-server host 192.168.2.1 accounting
switch(config)# radius-server host 192.168.2.1 key 0 MyKeyClr
switch(config)# radius-server host 192.168.2.1 key 7 MyKeyEnc
switch(config)# radius-server host 192.168.2.1 test idle-time 10
switch(config)# radius-server host 192.168.2.1 test username testuser
switch(config)# radius-server host 192.168.2.1 test password 2B9ka5
```

This example shows how to restore the default idle time for a specific RADIUS server:

```
switch(config)# no radius-server host 192.168.2.1 idle-time 10
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send feedback to nexus4K-docfeedback@cisco.com

radius-server key

To configure the global secret key that is used by all RADIUS servers to authenticate with the switch, use the **radius-server key** command. To disable the global key, use the **no** form of this command.

radius-server key [**0** | **7**] *key-value*

no radius-server key [**0** | **7**] *key-value*

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.
key-value	Preshared key. The maximum length is 63 characters.

Command Default

Clear text authentication.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 63 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 set the authentication key to AnyWord:

```
switch(config)# radius-server key AnyWord
```

This example shows how to set the authentication and encryption key to AnyWord. The 7 specifies that a hidden key will follow.

```
switch(config)# radius-server key 7 AnyWord
```

This example shows how to remove the encryption key from RADIUS authentication:

```
switch(config)# no radius-server key 7 AnyWord
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
radius-server host	Configures a RADIUS server host.
show radius-server	Displays RADIUS server information.

Send feedback to nexus4K-docfeedback@cisco.com

radius-server retransmit

To configure the maximum number of times for the switch to retry transmitting to a RADIUS server before reverting to local authentication, use the **radius-server retransmit** command. To restore the default configuration, 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 attempt.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The retransmit configuration is applied to all RADIUS servers.

Examples

This example shows how to specify a retransmit counter value of 3 times:

```
switch(config)# radius-server retransmit 3
```

This example shows how to restore the default retransmission count:

```
switch(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
radius-server host	Configures a RADIUS server host.
show radius-server	Displays RADIUS server information.

Send feedback to nexus4K-docfeedback@cisco.com

radius-server timeout

To configure the global timeout interval specifying how long to wait for a response from a RADIUS server before declaring a timeout failure, use the **radius-server timeout** command. To restore the default timeout value, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Command Default

1 second.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to how to set the interval timer to 30 seconds:

```
switch(config)# radius-server timeout 30
```

This example shows how to restore the default interval:

```
switch(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send feedback to nexus4K-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. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. The remark text 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
4.1(2)E1(1)	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.

If you do not specify a sequence number, the switch adds the remark to the end of the ACL and assigns it a sequence number that is 10 greater than the sequence number of the preceding rule.

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-lists
```

This example shows how to remove a remark in an IPv4 ACL:

```
switch(config-acl)# no remark This ACL denies the marketing department access to the lab
switch(config-acl)#
```

Send feedback to nexus4K-docfeedback@cisco.com

This example shows how to remove a remark in an IPv4 ACL using only the sequence number:

```
switch(config-acl)# no 100
switch(config-acl)#
```

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 feedback to nexus4K-docfeedback@cisco.com

resequence

To reassign sequence numbers to all rules in an access control list (ACL), use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name starting-number increment*

Syntax Description

access-list-type	Type of the ACL. Valid values for this argument are the following keywords: • **ip** • **mac**
access-list *access-list-name*	Specifies the name of the ACL. The name can be maximum 64 characters.
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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL. 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, no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch(config)# show ip access-lists ip-acl-01

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
```

Send feedback to nexus4K-docfeedback@cisco.com

```
IP access list ip-acl-01
        100 permit tcp 128.0.0.0/16 any eq www
        110 permit udp 128.0.0.0/16 any
        120 permit icmp 128.0.0.0/16 any eq echo
        130 deny igmp any any
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
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 feedback to nexus4K-docfeedback@cisco.com

role feature-group name

To create 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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch(config)# no role feature-group name MyGroup
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
feature	Configures features in a user role feature group.
show role feature-group	Displays the user role feature groups.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

A Cisco Nexus 4001I and Cisco Nexus 4005I switch provides the following default user roles:

- Network Administrator—Complete read-and-write access to the entire switch
- Complete read access to the entire switch

You cannot change or remove the default user roles.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to remove a user role:

```
switch(config-role)# no role name MyRole
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
interface policy deny	Configures the interface policy for the role.
show role	Displays the user roles.
username	Configures a user account.

Send feedback to nexus4K-docfeedback@cisco.com

Command	Description
vlan policy deny	Configures the VLAN policy for the role.
vrf policy deny	Configures the Virtual Private Network (VPN) routing and forwarding instance (VRF) policy for the role.

Send feedback to nexus4K-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. Valid values are 1 to 256. 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) Configures a read-only or read-and-write rule for a feature. The feature name can be 32 characters. **Note** Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
feature-group *group-name*	(Optional) Configures a read-only or read-and-write rule for a feature group. The group name can be 32 characters. **Note** Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.

Command Default

No default behavior or values.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

Send feedback to nexus4K-docfeedback@cisco.com

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.

To separate two or more commands in the *command-string*, press the **Space** key, and then press **;**. Example, config t ; role *.

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
```

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
copy running-config startup-config	Copies the running configuration to the startup configuration.
role feature-group name	Configures a user role feature group.
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.

Send feedback to nexus4K-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* | *hostname*}

no server {*ipv4-address* | *hostname*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
hostname	Server name. The maximum length is 256 characters.

Command Default

No default behavior or values.

Command Modes

Radius server group configuration

Tacacs+ server group configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure up to 64 servers in a server group.

Use the **aaa group server radius** command to enter radius server group configuration mode or **aaa group server tacacs+** command to enter tacacs+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

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

Examples

This example shows how to add a server to a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.2.1
```

This example shows how to delete a server from a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.2.1
```

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 192.168.2.2
```

Send feedback to nexus4K-docfeedback@cisco.com

This example shows how to delete a server from a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 192.168.2.2
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show aaa accounting** command and displays information about the AAA configuration:

```
switch# show aaa accounting
default: local
switch(config)#
```

Related Commands

Command	Description
aaa accounting default	Configures AAA methods for accounting.

Send feedback to nexus4K-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. Displays the configuration information when authentication login error message is enabled.
mschap	(Optional) Displays the authentication login Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) enable configuration.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show aaa authentication** command and displays information about the configured authentication parameters:

```
switch# show aaa authentication
         default: local
         console: group TacServer
switch(config)#
```

The following is sample output from the **show aaa authentication login error-enable** command and displays information about the authentication login error enable configuration:

```
switch# show aaa authentication login error-enable
disabled
switch(config)#
```

The following is sample output from the **show aaa authentication login mschap** command and displays information about the authentication login MS-CHAP configuration:

```
switch# show aaa authentication login mschap
disabled
switch(config)#
```

Related Commands

Send feedback to nexus4K-docfeedback@cisco.com

Command	Description
aaa authentication login console	Configures AAA console login authentication.
aaa authentication login default	Configures AAA default login authentication.
aaa authentication login error-enable	Enables AAA authentication failure messages to display on the console.
aaa authentication login mschap enable	Enables MS-CHAP authentication for logging in to the AAA servers.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable the TACACS+ feature on the switch by using the **feature tacacs+** command before you can display TACACS+ information.

Examples

The following is sample output from the **show aaa groups** command and displays information about the AAA groups:

```
switch# show aaa groups
radius
RadServer
tacacs
TacServer
switch#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server group information.
show tacacs-server	Displays TACACS+ server group information

Send feedback to nexus4K-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. The name can be maximum 64 characters.

Command Default

The switch shows all ACLs, unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show access-lists** command and displays information about the IPv4 and MAC ACLs configured on the switch:

```
switch# show access-lists

MAC access list 01-mac-acl
        10 permit any any ip cos 3
        20 permit any any vlan 5
        30 permit 00c0.4f03.0a72 0000.0000.0000 any aarp
        40 permit any 0060.3e00.0000 0000.0000.0000 ip vlan 3
        50 deny any any vines-echo cos 1
MAC access list 02-mac-acl
        10 deny any any ip vlan 2
IP access list 01-myacl
        10 deny tcp 192.168.1.37/16 192.168.1.176/16
IP access list acl2
        10 permit tcp any any
IP access list ip-acl-01
        1 remark This ACL permits UDP traffic
        21 permit udp 192.168.2.3/3 192.168.2.116/3
        41 permit tcp 192.168.3.23/12 192.168.3.176/12
switch#
```

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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show accounting log** command and displays information about the accounting log:

```
switch# show accounting log
```

The following is sample output from the **show accounting log 500** command and displays 500 bytes of the accounting log:

```
switch# show accounting log 500

Wed Aug  5 06:01:28 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
Wed Aug  5 06:10:06 2009:update:192.168.2.168@pts/0:root:configure terminal ; r
adius-server host myRad test username testuser password testpwd idle-time 10 (SU
CCESS)
Wed Aug  5 06:10:39 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
switch#
```

The following is sample output from the **show accounting log start-time** command and displays information about the accounting log starting at 16:00:00 on August 5, 2009:

```
switch# show accounting log start-time 2009 Aug 5 06:00:00

Wed Aug  5 06:01:06 2009:update:192.168.2.168@pts/0:root:tacacs+ disabled
```

Send feedback to nexus4K-docfeedback@cisco.com

```
Wed Aug  5 06:01:06 2009:update:192.168.2.168@pts/0:root:configure terminal ; n
o feature tacacs+ (SUCCESS)
Wed Aug  5 06:01:24 2009:update:192.168.2.168@pts/0:root:tacacs+ enabled
Wed Aug  5 06:01:24 2009:update:192.168.2.168@pts/0:root:configure terminal ; f
eature tacacs+ (SUCCESS)
Wed Aug  5 06:01:28 2009:update:192.168.2.168@pts/0:root:updated TACACS+ parame
ters for group:TacServer
Wed Aug  5 06:01:28 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
Wed Aug  5 06:10:06 2009:update:192.168.2.168@pts/0:root:configure terminal ; r
adius-server host myRad test username testuser password testpwd idle-time 10 (SU
CCESS)
Wed Aug  5 06:10:39 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
switch#
```

The following is sample output from the **show accounting log** command and displays information about the accounting log starting at 15:59:59 on August 3, 2009 and ending at 16:00:00 on August 5, 2009:

```
switch# show accounting log start-time 2009 Aug 3 15:59:59 end-time 2009 Aug 5 16:00:00
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

Send feedback to nexus4K-docfeedback@cisco.com

show interface counters storm-control

To view the storm-control levels set on the interface, use the **show interface counters** command.

show interface [**ethernet** *slot/port* | **port-channel** *number*] **counters storm-control**

Syntax Description

ethernet *slot/port*	(Optional) Specifies the Ethernet interface slot number and port number.
port-channel *number*	(Optional) Specifies the EtherChannel interface number.

Command Default

Displays the storm-control levels of all interfaces.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show interface counters storm-control** command and displays information about the storm-control levels set on the interfaces:

```
switch# show interface counters storm-control

--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth1/1          100.00          100.00          100.00                     0
Eth1/2           30.00          100.00          100.00                     0
Eth1/3          100.00          100.00          100.00                     0
Eth1/4          100.00          100.00          100.00                     0
Eth1/5          100.00          100.00          100.00                     0
Eth1/6          100.00          100.00          100.00                     0
Eth1/7          100.00          100.00          100.00                     0
Eth1/8          100.00          100.00          100.00                     0
Eth1/9          100.00          100.00          100.00                     0
Eth1/10         100.00          100.00          100.00                     0
Eth1/11         100.00          100.00          100.00                     0
Eth1/12         100.00          100.00          100.00                     0
Eth1/13         100.00          100.00          100.00                     0
Eth1/14         100.00          100.00          100.00                     0
Eth1/15         100.00          100.00          100.00                     0
Eth1/16         100.00          100.00          100.00                     0
Eth1/17         100.00          100.00          100.00                     0
Eth1/18         100.00          100.00          100.00                     0
Eth1/19         100.00          100.00          100.00                     0
Eth1/20         100.00          100.00          100.00                     0
switch#
```

The following is sample output from the **show interface ethernet 1/2 counters storm-control** command and displays information about the storm-control levels set on Ethernet interface 1/2:

```
switch# show interface ethernet 1/2 counters storm-control
```

Send feedback to nexus4K-docfeedback@cisco.com

```
--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth1/2           30.00          100.00          100.00                      0

switch#
```

Related Commands

Command	Description
storm-control	Sets the storm-control threshold value and blocks forwarding of unnecessary flooded traffic.
show running-config	Displays the configuration of the interfaces.

Send feedback to nexus4K-docfeedback@cisco.com

show ip access-lists

To display all IPv4 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. The name can be maximum 64 characters.

Command Default

The switch shows all IPv4 ACLs, unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show ip access-lists** command and displays information about the IPv4 ACLs configured on the switch:

```
switch# show ip access-lists

IP access list test
        10 permit ip 192.168.2.1/32 192.168.2.2/32

IP access list ip-acl-01
        10 permit ip 192.168.2.1/5 any
        20 permit tcp 192.168.2.23/16 192.168.2.176/16
        30 deny udp 192.168.3.25/12 192.168.3.27/15
switch#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

Send feedback to nexus4K-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. The name can be maximum 64 characters.

Command Default

The switch shows all MAC ACLs, unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show mac access-lists** command and displays information about the MAC ACLs configured on the switch:

```
switch# show mac access-lists

MAC access list 01-mac-acl
        10 permit any any ip cos 3
        20 permit any any vlan 5
        30 permit 00c0.4f03.0a72 0000.0000.0000 any aarp
        40 permit any 0060.3e00.0000 0000.0000.0000 ip vlan 3
        50 deny any any vines-echo cos 1
MAC access list 02-mac-acl
        10 deny any any ip vlan 2
switch#
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

Send feedback to nexus4K-docfeedback@cisco.com

show radius-server

To display RADIUS server information, use the **show radius-server** command.

show radius-server [{*hostname* | *ipv4-address*} | **directed-request** | **groups** [*group-name*] | **sorted** | **statistics** {*hostname* | *ipv4-address*}]

Syntax Description

hostname	(Optional) RADIUS server Domain Name System (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) RADIUS server IPv4 address in the *A.B.C.D* format.
directed-request	(Optional) Displays the directed request configuration.
groups [*group-name*]	(Optional) Displays information about the configured RADIUS server groups or a specific RADIUS server group.
group-name	(Optional) Name of the RADIUS server group. The name is alphanumeric and case-sensitive. The name can be maximum 64 characters.
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

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show radius-server** command and displays information about the RADIUS servers configured on the switch:

```
switch# show radius-server
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:5
source interface:any available
total number of servers:2

following RADIUS servers are configured:
        192.168.2.168:
                available for authentication on port:1812
                available for accounting on port:1813
```

Send feedback to nexus4K-docfeedback@cisco.com

```
        host1:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
switch#
```

The following is sample output from the **show radius-server 192.268.2.168** command and displays information about the specified RADIUS server:

```
switch# show radius-server 192.168.2.168
192.168.2.168:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
                idle time:10
                test user:testuser
                test password:********
switch#
```

The following is sample output from the **show radius-server directed-request** command and displays information about the RADIUS directed request configuration:

```
switch# show radius-server directed-request
disabled
switch#
```

The following is sample output from the **show radius-server groups** command and displays information about the RADIUS server groups:

```
switch# show radius-server groups
total number of groups:1

following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
                deadtime is 0
switch#
```

The following is sample output from the **show radius-server groups** command and displays information about the specified RADIUS server group:

```
switch# show radius-server groups RadServer
group RadServer:
                server: host1 on auth-port 1812, acct-port 1813
                deadtime is 5
switch#
```

The following is sample output from the **show radius-server sorted** command and displays information about the RADIUS servers configured on the switch, sorted by radius server names:

```
switch# show radius-server sorted
timeout value:5
retransmission count:1
deadtime value:5
source interface:any available
total number of servers:2

following RADIUS servers are configured:
        192.168.2.168:
                available for authentication on port:1812
                available for accounting on port:1813
        host1:
                available for authentication on port:1812
                available for accounting on port:1813
```

Send feedback to nexus4K-docfeedback@cisco.com

```
switch#
```

The following is sample output from the **show radius-server statistics** command and displays the statistics for a specified RADIUS servers:

```
switch# show radius-server statistics 192.168.2.168
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
switch#
```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

Send feedback to nexus4K-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. The name can be maximum 16 characters.

Command Default

Displays information for all user roles.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show role name** command and displays information about the specified user role:

```
switch# show role name MyRole
```

The following is sample output from the **show role** command and displays information about all user roles:

```
switch# show role
Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: myRole
  Description: User-defined user who can operate the switch
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 3,5
  Interface policy: deny
  Permitted interfaces:
  Ethernet1/3,Ethernet1/5
  Vrf policy: deny
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  Permitted vrfs: management
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  5       permit  command                         configure terminal ; vlan *
  4       permit  read-write  feature-group       myGroup
  3       deny    read-write  feature             arp
  2       deny    command                         clear users
  1       permit  read        feature             ping

switch#
```

Related Commands

Command	Description
role name	Configures user roles.

Send feedback to nexus4K-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. The name can be maximum 16 characters.

Command Default

Displays a list of user role feature names.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show role feature** command and displays information about the user role features:

```
switch# show role feature
feature: aaa
feature: access-list
feature: arp
feature: callhome
feature: cdp
feature: install
feature: l3vm
feature: license
feature: ping
feature: platform
feature: radius
feature: snmp
feature: syslog
feature: tacacs
feature: eth-span
feature: ethanalyzer
feature: spanning-tree
feature: vlan
switch#
```

The following is sample output from the **show role feature detail** command and displays detailed information about the user role features:

```
switch# show role feature detail
feature: aaa
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
feature: access-list
  show ip access-lists *
  show ipv6 access-lists *
  show mac access-lists *
  show arp access-lists *
  show vlan access-map *
  show vlan access-list *
  show vlan filter *
  config t ; ip access-list *
  config t ; ipv6 access-list *
  config t ; mac access-list *
  config t ; arp access-list *
  config t ; vlan access-map *
  config t ; time-range *
  config t ; resequence *
  config t ; errdisable detect cause acl-exception
  config t ; object-group *
  config t ; interface * ; ip access-group *
  config t ; interface * ; ip port access-group *
  config t ; interface * ; ipv6 traffic-filter *
  config t ; interface * ; ipv6 port traffic-filter *
  config t ; interface * ; errdisable port detect cause acl-exception
  config s ; ip access-list *
  config s ; ipv6 access-list *
  config s ; mac access-list *
--More--
switch#
```

The following is sample output from the **show role feature name** command and displays detailed information about the specific user role feature:

```
switch# show role feature name vlan
feature: vlan
  show vlan *
  config t ; vlan *
  vlan *
  clear vlan *
  debug vlan *
  show vlan-mgr *
  config t ; vlan-mgr *
  vlan-mgr *
  clear vlan-mgr *
  debug vlan-mgr *
  show pvlan *
  config t ; pvlan *
  pvlan *
  clear pvlan *
  debug pvlan *
switch#
```

Related Commands

Command	Description
feature (user role)	Configures a feature in a user role feature group.

Send feedback to nexus4K-docfeedback@cisco.com

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show role feature-group** command and displays information about the user role feature groups:

```
switch# show role feature-group

feature group: myGroup
feature: aaa
feature: radius
feature: tacacs
switch#
```

The following is sample output from the **show role feature-group detail** command and displays detailed information about the user role feature groups:

```
switch# show role feature-group detail
```

The following is sample output from the **show role feature-group name** command and displays information about 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 feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config aaa** command and displays the configured AAA information in the running configuration:

```
switch# show running-config aaa
version 4.1(2)E1(1)
aaa authentication login default group radius
radius-server directed-request
tacacs-server directed-request

switch#
```

The following is sample output from the **show running-config aaa all** command and displays the detailed AAA configuration information in the running configuration:

```
switch# show running-config aaa all
version 4.1(2)E1(1)
no snmp-server enable traps aaa server-state-change
aaa authentication login default group radius
aaa accounting default local
aaa user default-role
no aaa authentication login error-enable
no aaa authentication login mschap enable
no aaa authentication login ascii-authentication
radius-server directed-request
no tacacs-server directed-request
tacacs-server directed-request

switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show aaa accounting	Displays AAA accounting configuration information.
show aaa authentication	Displays AAA authentication configuration information.
show startup-config aaa	Displays AAA configuration in the startup configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config radius** command and displays information about the RADIUS server configuration:

```
switch# show running-config radius
version 4.1(2)E1(1)
radius-server host 192.168.2.168 authentication accounting
radius-server host host1 key 7 "MyKeyEnc" authentication accounting
radius-server host host1 test username testuser password testpwd idle-time 10
radius-server host myRad key 7 "KkxPwy" authentication accounting
aaa group server radius RadServer
    server host1
    deadtime 5

switch#
```

The following is sample output from the **show running-config radius all** command and displays detailed information about RADIUS server groups and host configurations:

```
switch# show running-config radius all
version 4.1(2)E1(1)
radius-server timeout 5
radius-server retransmit 1
radius-server deadtime 0
no ip radius source-interface
radius-server host 192.168.2.168 auth-port 1812 acct-port 1813 authentication acco
unting
radius-server host 192.168.2.168 test username test password test idle-time 0
radius-server host host1 key 7 "MyKeyEnc" auth-port 1812 acct-port 1813 authenti
cation accounting
radius-server host host1 test username testuser password testpwd idle-time 10
radius-server host myRad key 7 "KkxPwy" auth-port 1812 acct-port 1813 authentica
tion accounting
radius-server host myRad test username test password test idle-time 0
aaa group server radius radius
```

Send feedback to nexus4K-docfeedback@cisco.com

```
    server 192.168.2.168
    server host1
    server myRad
    deadtime 0
    use-vrf default
    no source-interface
aaa group server radius RadServer
    server host1
    deadtime 5
    use-vrf default
    no source-interface

switch#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS information.
show startup-config radius	Displays RADIUS server in the startup configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config security** command and displays the running configuration information about the user account, SSH server, and Telnet server:

```
switch# show running-config security
version 4.1(2)E1(1)
feature telnet
no feature ssh

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role networ
-operator
username admin password 5 $1$zkTYLs/y$sOecMEkhsnJT8Lu8rbPAQ/  role network-admi
username USERID password 5 $1$8UHo5rdt$6zLdUqn4dr3Aqk0DFyBlq.  role network-ope
ator

banner motd #Nexus 4000 Switch#

switch#
```

The following is sample output from the **show running-config security all** command and displays the detailed security information available in the running configuration.

```
switch# show running-config security all
version 4.1(2)E1(1)
feature telnet
no feature ssh

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network
-operator
username admin password 5 $1$qBkDwg9Y$JLTReKR3IWscqEAXpPLb5/  role network-admin
username USERID password 5 $1$fDVBuiJu$MQ3JiBFO7AAFqnzSwMhEE.  role network-oper
ator
password strength-check
```

Send feedback to nexus4K-docfeedback@cisco.com

```
banner motd #Nexus 4000 Switch#

ssh key rsa 1024
no ssh key dsa

switch#
```

Related Commands

Command	Description
show startup-config security	Displays user accounts, SSH server, and Telnet server configuration information in the startup configuration.

Send feedback to nexus4K-docfeedback@cisco.com

show running-config tacacs+

To display TACACS+ configuration information in the running configuration, use the **show running-config tacacs+** command.

show running-config tacacs+ [**all**]

Syntax Description

all	(Optional) Displays default TACACS+ configuration information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable the TACACS+ feature on the switch by using the **feature tacacs+** command before you can display TACACS+ information.

Examples

The following is sample output from the **show running-config tacacs+** command and displays information about the TACACS+ configuration:

```
switch# show running-config tacacs+
version 4.1(2)E1(1)
feature tacacs+

tacacs-server deadtime 5
tacacs-server host tacacs2 key 7 "DjcPwy" timeout 5
tacacs-server host tacacs2 test idle-time 10
tacacs-server host tacacs3 key 7 "DjcPwy"
aaa group server tacacs+ tacacs
aaa group server tacacs+ TacServer
    server tacacs2
    deadtime 20
switch#
```

The following is sample output from the **show running-config tacacs+ all** command and displays detailed information about the TACACS+ configuration:

```
switch# show running-config tacacs+ all
version 4.1(2)E1(1)
feature tacacs+

tacacs-server timeout 5
tacacs-server deadtime 5
no ip tacacs source-interface
tacacs-server host tacacs2 key 7 "DjcPwy" port 49 timeout 5
tacacs-server host tacacs2 test username test password test idle-time 10
tacacs-server host tacacs3 key 7 "DjcPwy" port 49
```

Send feedback to nexus4K-docfeedback@cisco.com

```
tacacs-server host tacacs3 test username test password test idle-time 0
aaa group server tacacs+ tacacs
    use-vrf default
    no source-interface
aaa group server tacacs+ TacServer
    server tacacs2
    deadtime 20
    use-vrf default
    no source-interface

switch#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+ on the switch.
show startup-config tacacs+	Displays TACACS+ server information in the startup configuration.
show tacacs-server	Displays TACACS+ server information.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command is available only when SSH is enabled using the **ssh server enable** command.

Examples

The following is sample output from the **show ssh key** command and displays information about the SSH server keys:

```
switch# show ssh key
**************************************
rsa Keys generated:Tue Aug  4 22:18:57 2009

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAop9LIBbT2mydCBOpt8PZ9jYZuUiVqyLBcL7ogcOpuN4M
Ju+Y6pa7v3nvwcUQ8LRxq6pVL5lFO5heU/RV0sU4vaWLY1lMWuAIgIcLY7YX2zv7Pte6gW2Y8jVVI3ce
jt09OffM2JiHc/KJbPfchzC7+FJJ+s5ivKodYG4bnL1gBw0=

bitcount:1024
fingerprint:
c1:e4:a1:27:ea:01:52:fd:b1:a9:a1:ca:c4:aa:53:53
**************************************
dsa Keys generated:Wed Aug  5 09:23:37 2009

ssh-dss AAAAB3NzaC1kc3MAAACBAKQrOK6RvuQ9NvUnXU8xnmmZkguTjT84RlE9piyRMcTNWYsLsRi9
TJS1mHNnEk5h8+4Cfi16BRFgsoI952tzff4j+YunmuxXxuvZ3t37L8j8wB/gTIU2QAcSOM8A3d2pjcMj
d7VMW1vilkJfGDfTJHmToTR5vCHka+yZbLqEn7/tAAAAFQCGcIm8L9EozxDNGcZUA4D2C3120wAAAIBs
7oVB5ESlmYKcIWUbear54nqnbD5d9KYH1rtnIUIp8k6vACYMDfnXQv/zMdZS3s/8YCqGU8XD1dl52Lw+
JVMtHVgyqL2t9O9XFe2ew61kqHh1jbJFmmTuW+iUBYZshTDn5N8Ujw2Nrpu3+j1BFsTIV//mIC5Dzcpf
D7+5pNMZ5wAAAIBASR/ooYfMPJAWTrSRwifes5ByEffUn1lnes4/NxwnqMNLnMhMuuYE3t/X2oZXNI/k
EIxNyQ0X08mIktVRdSZQ7lITkWtYYQPA/Ua91bevFzgiwWZam4aswwHOHMO4bd1guVyQGngBjON3iTs5
KvemLHjVT3yiri9aDdvBfw78XQ==

bitcount:1024
fingerprint:
1a:8a:66:44:27:35:d6:8e:93:89:5b:5b:02:31:9c:60
**************************************
switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
ssh key	Configures the SSH server key.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable SSH on the switch by using the **feature ssh** command.

Examples

The following is sample output from the **show ssh server** command and displays information about the SSH server status:

```
switch# show ssh server
ssh version 2 is enabled
switch#
```

Related Commands

Command	Description
feature ssh	Enables SSH on the switch.
ssh server enable	Enables the SSH server.

Send feedback to nexus4K-docfeedback@cisco.com

show startup-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the startup configuration, use the **show startup-config aaa** command.

show startup-config aaa

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the AAA running configuration to the startup configuration before you can display the AAA startup configuration information.

Examples

The following is sample output from the **show startup-config aaa** command and displays information about the AAA available in the startup configuration:

```
switch# show startup-config aaa
version 4.1(2)E1(1)
aaa authentication login default group radius
radius-server directed-request
tacacs-server directed-request

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config aaa	Displays AAA configuration information in the running configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the RADIUS server running configuration to the startup configuration before you can display the RADIUS server startup configuration information.

Examples

The following is sample output from the **show startup-config radius** command and displays information about the RADIUS server available in the startup configuration:

```
switch# show startup-config radius
version 4.1(2)E1(1)
radius-server host 192.168.2.168 authentication accounting
radius-server host host1 key 7 "MyKeyEnc" authentication accounting
radius-server host host1 test username testuser password testpwd idle-time 10
radius-server host myRad key 7 "KkxPwy" authentication accounting
radius-server host myRad test username testuser password testpwd idle-time 10
aaa group server radius RadServer
    server host1
    deadtime 5

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config radius	Displays the RADIUS server information in the running configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the RADIUS server running configuration to the startup configuration before you can display the RADIUS server startup configuration information.

Examples

The following is sample output from the **show startup-config security** command and displays information about the user account, SSH server, and Telnet server available in the startup configuration:

```
switch# show startup-config security
version 4.1(2)E1(1)
feature telnet
no feature ssh

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network
-operator
username admin password 5 $1$qBkDwg9Y$JLTReKR3IWscqEAXpPLb5/  role network-admin
username USERID password 5 $1$fDVBuiJu$MQ3JiBFO7AAFqnzSwMhEE.  role network-oper
ator

banner motd #Nexus 4000 Switch#

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config security	Displays the user account, SSH server, Telnet server information in the running configuration.

Send feedback to nexus4K-docfeedback@cisco.com

show startup-config tacacs+

To display TACACS+ configuration information in the startup configuration, use the **show startup-config tacacs+** command.

show startup-config tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the RADIUS server running configuration to the startup configuration before you can display the RADIUS server startup configuration information.

Examples

The following is sample output from the **show startup-config tacacs+** command and displays information about the TACACS+ server configuration available in the startup configuration:

```
switch# show startup-config tacacs+
version 4.1(2)E1(1)
feature tacacs+

tacacs-server deadtime 5
tacacs-server host tacacs2 key 7 "DjcPwy" timeout 5
tacacs-server host tacacs2 test idle-time 10
tacacs-server host tacacs3 key 7 "DjcPwy"
aaa group server tacacs+ tacacs
aaa group server tacacs+ TacServer
    server tacacs2
    deadtime 20

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config tacacs+	Displays the TACACS+ server information in the running configuration.

Send feedback to nexus4K-docfeedback@cisco.com

show tacacs-server

To display TACACS+ server information, use the **show tacacs-server** command.

show tacacs-server [{*hostname* | *ipv4-address*} | **directed-request** | **groups** | **sorted** | **statistics]**

Syntax Description

hostname	(Optional) TACACS+ server Domain Name System (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) TACACS+ server IPv4 address in the *A.B.C.D* 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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you can display TACACS+ information.

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.

Examples

The following is sample output from the **show tacacs-server** command and displays information about the TACACS+ servers:

```
switch# show tacacs-server
timeout value:5
deadtime value:5
source interface:any available
total number of servers:1

following TACACS+ servers are configured:
        tacacs2:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

The following is sample output from the **show tacacs-server** command and displays information about a specified TACACS+ server:

```
switch# show tacacs-server tacacs2
tacacs2:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
                idle time:10
                test user:test
                test password:********
switch#
```

The following is sample output from the **show tacacs-server directed-request** command and displays information about the TACACS+ directed request configuration:

```
switch# show tacacs-server directed-request
disabled
switch#
```

The following is sample output from the **show tacacs-server groups** command and displays information about the TACACS+ server groups:

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group tacacs:
                deadtime is 0
        group TacServer:
                server tacacs2 on port 49
                deadtime is 20
                vrf is default
switch#
```

The following is sample output from the **show tacacs-server groups** command and displays information about a specified TACACS+ server group:

```
switch# show tacacs-server groups TacServer
group TacServer:
                server tacacs2 on port 49
                deadtime is 20
                vrf is default
switch#
```

The following is sample output from the **show tacacs-server sorted** command and displays information about the TACACS+ servers, sorted by server name:

```
switch# show tacacs-server sorted
timeout value:5
deadtime value:5
source interface:any available
total number of servers:2

following TACACS+ servers are configured:
        tacacs2:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
        tacacs3:
                available on port:49
                TACACS+ shared secret:********
switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

The following is sample output from the **show tacacs-server statistics** command and displays the statistical information for a specified TACACS+ server:

```
switch# show tacacs-server statistics tacacs2
Server is dead since 0 hrs, 0 min, 0 sec

Monitoring Statistics
        Time in previous state: 0 hrs, 10 min, 2 sec
        Number of times dead: 1
        Total time in dead state: 0 hrs, 0 min, 0 sec

Authentication Statistics
        failed transactions: 1
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
switch#
```

Related Commands

Command	Description
show running-config tacacs+	Displays the TACACS+ information in the running configuration file.
show startup-config tacacs+	Displays TACACS+ server information in the startup configuration.
tacacs-server host	Configures TACACS+ server parameters.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show telnet server** command and displays information about the Telnet server status:

```
switch# show telnet server
telnet service enabled
switch#
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

Send feedback to nexus4K-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

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples The following is sample output from the **show user-account** command and displays information about the user accounts defined on the switch:

```
switch# show user-account
user:root
        this user account has no expiry date
        roles:network-operator
user:adminbackup
        this user account has no expiry date
        roles:network-operator
user:admin
        this user account has no expiry date
        roles:network-admin
        ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxXkib5JVXsM/GVJtYeZS
Gah8IR20OsqnN0QZ166wtR/b0MDPv1MuMuJl1suzV2NkohuH9n55jTnwaFovuw6F238pkbhzJ6YdQjMK
67g+YDSAMjB3Ywh1lA+HYIv3juFVEiGP4daXMPFFQe5FHCZMDHWrzSFpp8oa5asfoasCI2U=
user:USERID
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-dss AAAAB3NzaC1kc3MAAACBAM694BlguDIyzxeqcry8gEu1Wke4
vB+TtVO7T+oAm1KpWM0GAtSr7ANSjlcqKyNGiosNzZ/41FDWunjBJs4xYCbAJK7/IhLYYHeaSKzPH5h3
StFJD6U3u8HLHfeaMaogzAv8eUA6SLQCDBDfHJPWGcsDguItCanUTBmqobVDazIVAAAAFQCJJio5hvUY
xYxFSDUSbzdtXYWpgwAAAIASv6eEMXmR5M5hlCmyE3NPCiTHvrCWwaqROet6AMI8IXZgD7XfGnnYPMTn
nfVTPJZnaCTjL+fH06Bjl0nBLmvsDE1Hcndrn3ldeJwolVtmcjDYBmUUdqncxn48qxaxSsNc5NrR8Ias
Zbo02GJDa8tduhLAKRJTZ/xs9GgKUieITAAAAIA3q0tmhwnRgHJMOb3Y9A3rUewKO6fMTqBbLh14bs+m
Avw7h7kOwYJcmWpYVk58Svrqy/asMBY19PCyXn7NjaIxQZLEyA3Ep50iSvbydXqbkVyX7D1GSjV4H+ck
dZkj5pb9Fpx2YuNXvrF9vaoLUdI4Tu2FosElijrO/FI8artF8A==

switch#
```

The following is sample output from the **show user-account user1** command and displays information about a specific user account:

Send feedback to nexus4K-docfeedback@cisco.com

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-dss AAAAB3NzaC1kc3MAAACBAM694BlguDIyzxeqcry8gEu1Wke4
vB+TtVO7T+oAm1KpWM0GAtSr7ANSjlcqKyNGiosNzZ/41FDWunjBJs4xYCbAJK7/IhLYYHeaSKzPH5h3
StFJD6U3u8HLHfeaMaogzAv8eUA6SLQCDBDfHJPWGcsDguItCanUTBmqobVDazIVAAAAFQCJJio5hvUY
xYxFSDUSbzdtXYWpgwAAAIASv6eEMXmR5M5hlCmyE3NPCiTHvrCWwaqROet6AMI8IXZgD7XfGnnYPMTn
nfVTPJZnaCTjL+fH06Bjl0nBLmvsDE1Hcndrn3ldeJwolVtmcjDYBmUUdqncxn48qxaxSsNc5NrR8Ias
Zbo02GJDa8tduhLAKRJTZ/xs9GgKUieITAAAAIA3q0tmhwnRgHJMOb3Y9A3rUewKO6fMTqBbLh14bs+m
Avw7h7kOwYJcmWpYVk58Svrqy/asMBY19PCyXn7NjaIxQZLEyA3Ep50iSvbydXqbkVyX7D1GSjV4H+ck
dZkj5pb9Fpx2YuNXvrF9vaoLUdI4Tu2FosElijrO/FI8artF8A==
switch#
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
username	Configures a user account.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show users** command and displays information about the users currently logged on the switch:

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    ttyS0        Aug 10 04:49 03:43        2736
admin    pts/1        Aug 10 07:38   .          3952 (192.168.2.168) *
switch(config)#
```

Related Commands

Command	Description
clear user	Logs out a specific user.
username	Creates and configures a user account.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show vlan access-list** command and displays information about the ACLs associated with the specified VLAN access map:

```
switch# show vlan access-list vlan-map-01

VLAN access-map vlan-map-01 1
        IP access list ip-acl-01
        1 remark This ACL permits UDP traffic
        21 permit udp 192.168.2.37/3 192.168.2.176/3
        41 permit tcp 192.168.5.23/12 192.168.5.176/12
switch#
```

Related Commands

Command	Description
mac access-list	Create or configures a MAC ACL.
show access-lists	Displays information about how a VLAN access map is applied.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
vlan access-map	Configures a VLAN access map.

Send feedback to nexus4K-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

Command History

Release	Modification
4.1(2)E1(1)	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

The following is sample output from the **show vlan access-map** command and displays information about a specific VLAN access map:

```
switch# show vlan access-map vlan-map-01

Vlan access-map vlan-map-01 1
        match ip: ip-acl-01
        action: forward
        statistics per-entry

switch#
```

The following is sample output from the **show vlan access-map** command and displays information about all VLAN access maps configured on the switch:

```
switch# show vlan access-map
```

Related Commands

Command	Description
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 feedback to nexus4K-docfeedback@cisco.com

show vlan filter

To display information about the 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

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show vlan filter** command and displays information about the instances of VLAN access maps that are applied to VLANs:

```
switch# show vlan filter

vlan map vlan-map-01:
        Configured on VLANs:    3
switch#
```

Related Commands

Command	Description
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 feedback to nexus4K-docfeedback@cisco.com

ssh

To start a Secure Shell (SSH) session using IPv4 to connect to remote devices, 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 host.
hostname	Hostname of the remote host.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The VRF name can be one of the following: • **chassis-management** • **default** • **management**

Command Default

Default VRF.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to create an SSH session using IPv4:

```
switch# ssh root@192.168.2.168 vrf management
```

Related Commands

Command	Description
show running-config security	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.

Send feedback to nexus4K-docfeedback@cisco.com

ssh key

To create a Secure Shell (SSH) server key, use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies the Digital System Algrorithm (DSA) SSH server key.
force	(Optional) Forces the generation of a DSA SSH key even if previous ones are present.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048.

Command Default

1024-bit length.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

Examples

This example shows how to create an SSH server key using RSA with the default key length:

```
switch(config)# ssh key rsa
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch(config)# ssh key rsa 768
```

This example shows how to replace an SSH server key using DSA with the force option:

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

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

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

Send feedback to nexus4K-docfeedback@cisco.com

```
switch(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config security	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh key	Displays the SSH server key information.
show ssh server	Displays the SSH server configuration.
ssh server enable	Enables the SSH server.

Send feedback to nexus4K-docfeedback@cisco.com

ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	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 configuration.

Send feedback to nexus4K-docfeedback@cisco.com

statistics per-entry

To collect statistics for each ACL entry, use the **statistics per-entry** command. To remove statistics, use the **no** form of this command.

statistics per-entry

no statistics per-entry

Syntax Description

This command has no arguments or keywords.

Command Default

No statistics are collected.

Command Modes

Vlan access-map configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to collect statistics for each ACL entry:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# statistics per-entry
switch(config-access-map)#
```

This example shows how to remove statistics:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# no statistics per-entry
switch(config-access-map)#
```

Related Commands

Command	Description
match	Specifies an access control list (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.

Send feedback to nexus4K-docfeedback@cisco.com

storm-control

To set the storm-control threshold value and block forwarding of unnecessary flooded traffic on the interface, use the **storm-control level** command. To turn off storm control and restore the default threshold, 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 1 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
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

A traffic storm occurs when packets flood the interface, creating excessive traffic and degrading network performance. The traffic storm control (also called traffic suppression) feature prevents interface ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

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 interface 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.

Send feedback to nexus4K-docfeedback@cisco.com

Examples

This example shows how to enable multicast traffic storm control on Ethernet interface 1/2 and how to configure the traffic storm control level at 70.5 percent:

```
switch(config)# interface ethernet 1/2
switch(config-if)# storm-control multicast level 70.5
```

This example shows how to limit the threshold of broadcast traffic to 30 percent:

```
switch(config-if)# storm-control broadcast level 30
```

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 counters storm-control	Displays the total number of packets discarded for all three traffic storm control modes, on all interfaces or on the specified interface.
show running-config	Displays the configuration of the interface.

Send feedback to nexus4K-docfeedback@cisco.com

tacacs-server deadtime

To set a global periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To restore the default dead-time interval, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

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

Command Default

0 minutes.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 global 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 feedback to nexus4K-docfeedback@cisco.com

tacacs-server directed-request

To allow users 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

Command History

Release	Modification
4.1(2)E1(1)	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	Displays a directed request TACACS+ server configuration.

Send feedback to nexus4K-docfeedback@cisco.com

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command. To revert to the defaults, use the **no** form of this command.

tacacs-server host {*hostname* | *ipv4-address*} [**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*} [**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 System (DNS) name. The maximum character size is 256.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
key	(Optional) Configures the shared secret key of the TACACS+ server.
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 username 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.

Command Modes

Configuration

Send feedback to nexus4K-docfeedback@cisco.com

Command History

Release	Modification
4.1(2)E1(1)	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 the server IP address or hostname as a TACACS+ server host:

```
switch(config)# tacacs-server host tacacs2
```

This example shows how to configure a TCP port other than port 49 (the default for TACACSS+ requests):

```
switch(config)# tacacs-server host tacacs3 port 2
```

This example shows how to configure periodic monitoring of a TACACS+ host:

```
switch(config)# tacacs-server host tacacs3 test username user1 password a3z9yjqz7
idle-time 3
switch(config)#
```

This example shows how to set the timeout interval for a specific TACACS+ host:

```
switch(config)# tacacs-server host tacacs3 timeout 10
```

This example shows TACACS+ configuration:

```
switch(config)# tacacs-server host tacacs2 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs2 test idle-time 10
switch(config)# tacacs-server host tacacs2 test username tester
switch(config)# tacacs-server host tacacs2 test password 2B9ka5
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server configuration.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To restore the default global timeout value, 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

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

telnet

To create a Telnet session using IPv4 on a 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 virtual routing and forwarding (VRF) name to use for the Telnet session. The VRF name can be one of the following: • **chassis-management** • **default** • **management**

Command Default

Port 23 is the default port.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

```
switch# telnet 192.168.2.168 vrf management
```

Related Commands

Command	Description
feature telnet	Enables Telnet on the switch.
show running-config security	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.
show telnet server	Displays the Telnet server status.
telnet server enable	Enables the Telnet server.

Send feedback to nexus4K-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

Enabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable the Telnet server:

```
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch(config)# no telnet server enable
```

Related Commands

Command	Description
copy running-config startup-config	Copies thee changes made in the running configuration to the startup configuration.
show telnet server	Displays the Telnet server status.

Send feedback to nexus4K-docfeedback@cisco.com

use-vrf

To specify a virtual routing and forwarding (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

No default behavior or values.

Command Modes

Radius server group configuration

Tacacs+ server group configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-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.
show vrf	Displays VRF information.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.

Send feedback to nexus4K-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** [**0** | **5**] *password* | **role** *role-name* | **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	(Optional) Specifies a password for the account. The default is no password.
0	(Optional) Specifies that the password that follows should be in clear text.
5	(Optional) Specifies that the password that follows should be encrypted.
password	Password for the user. The maximum length is 64 characters.
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 for SSH authentication.
key	SSH key string.
filename *filename*	Specifies the name of a file that contains the SSH key string. The filename must be in the Cisco NX-OS file system format, *filesystem*:[/*directory*][/*filename*]. Table 1-4 lists URL prefix keywords for local writable storage file systems.

Command Default

No expiration date, password, or SSH key.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch accepts only strong passwords. The characteristics of a strong password include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words

Send feedback to nexus4K-docfeedback@cisco.com

- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Note Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, the password cannot include the quotation mark (" or '), vertical bar (|), or right angle bracket (>) characters at the beginning of the password.

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

Examples

This example shows how to create a user account:

```
switch(config)# username user1 password Ci5co@321
```

This example shows how to configure the SSH key for a user account:

```
switch(config)# username user1 sshkey ssh-dss
AAAAB3NzaC1kc3MAAACBAM694BlguDIyzxeqcry8gEu1Wke4vB+TtVO7T+oAm1KpWM0GAtSr7ANSjlcqKyNGiosNzZ
/41FDWunjBJs4xYCbAJK7/IhLYYHeaSKzPH5h3StFJD6U3u8HLHfeaMaogzAv8eUA6SLQCDBDfHJPWGcsDguItCanU
TBmqobVDazIVAAAAFQCJJio5hvUYxYxFSDUSbzdtXYWpgwAAAIASv6eEMXmR5M5hlCmyE3NPCiTHvrCWwaqROet6AM
I8IXZgD7XfGnnYPMTnnfVTPJZnaCTjL+fH06Bjl0nBLmvsDE1Hcndrn3ldeJwolVtmcjDYBmUUdqncxn48qxaxSsNc
5NrR8IasZbo02GJDa8tduhLAKRJTZ/xs9GgKUieITAAAAIA3q0tmhwnRgHJMOb3Y9A3rUewKO6fMTqBbLh14bs+mAv
w7h7kOwYJcmWpYVk58Svrqy/asMBY19PCyXn7NjaIxQZLEyA3Ep50iSvbydXqbkVyX7D1GSjV4H+ckdZkj5pb9Fpx2
YuNXvrF9vaoLUdI4Tu2FosElijrO/FI8artF8A==
```

This example shows how to configure the SSH key for a user account using a key stored in the file system:

```
switch(config)# username user1 sshkey file bootflash:key_file
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show user-account	Displays the user account configuration.

Send feedback to nexus4K-docfeedback@cisco.com

vlan access-map

To create a VLAN access map or to configure an existing VLAN access map, use the **vlan access-map** command. To remove a VLAN access map, use the **no** form of this command.

vlan access-map *map-name*

no vlan access-map *map-name*

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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:

```
switch(config)# vlan access-map vlan-map-01
switch(config-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 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 feedback to nexus4K-docfeedback@cisco.com

vlan filter

To apply a VLAN access map to one or more VLANs, use the **vlan filter** command. To remove 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. The name can be maximum 64 characters.
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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	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 feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
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 feedback to nexus4K-docfeedback@cisco.com

vlan policy deny

To deny access to a VLAN and 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
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter vlan policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

This example shows how to revert to the default VLAN policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
permit vlan	Specifies a range of VLANs that the role can access.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Send feedback to nexus4K-docfeedback@cisco.com

vrf policy deny

To deny access to a Virtual Private Network (VPN) routing and forwarding instance (VRF) and enter 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

No default behavior or values.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter vrf policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

This example shows how to revert to the default VRF policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
permit vrf	Specifies a range of VRFs that the role can access.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.



Send feedback to nexus4K-docfeedback@cisco.com

CHAPTER 6

FCoE Initialization Protocol Snooping Commands

This chapter describes the Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) Snooping commands available on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

fip-snooping enable

To enable FIP snooping on a VLAN, use the **fip-snooping enable** command. To disable FIP snooping on a VLAN, use the **no** form of this command.

fip-snooping enable

no fip-snooping enable

Syntax Description

This command has no arguments or keywords.

Command Default

FIP snooping is disabled on VLANs.

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable FIP snooping on the switch by using the **feature fip-snooping** command. The commands for configuring FIP snooping on VLANs are not visible until you enable this feature on the VLANs.

Examples

This example shows how to enable the FIP-snooping feature on a VLAN:

```
switch(config)# vlan 100
switch(config-vlan)# fip-snooping enable
switch(config-vlan)#
```

This example shows how to disable the FIP-snooping feature on a VLAN:

```
switch(config-vlan)# no fip-snooping enable
switch(config-vlan)#
```

Related Commands

Command	Description
fip-snooping	Enables FIP snooping on the switch.
switchport mode trunk	Changes an interface mode to trunk.
switchport trunk allowed vlan	Configures a VLAN for the switch-port trunk.

Send feedback to nexus4K-docfeedback@cisco.com

fip-snooping fc-map

To configure the FCoE MAC Address Prefix (FC-MAP) value associated with the FIP snooping VLAN, use the **fip-snooping fc-map** command. To remove the FC-MAP configuration from a VLAN, use the **no** form of this command.

fip-snooping fc-map *fc-map-value*

no fip-snooping fc-map

Syntax Description

fc-map-value	Specifies the FC-MAP value used by the FCoE Forwarder (FCF). If the FC-MAP value is not known, use a definite FC-MAP value of 0x0efc00.

Command Default

FC-MAP value is zero.

Command Modes

Vlan configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable FIP snooping on the VLAN by using the **fip-snooping enable** command. The commands for configuring FIP snooping on a VLAN are not visible until you enable this feature.

The FC-MAP is configured for each VLAN and is used to associate the FCoE Node (ENode).

Examples

This example shows how to configure FIP-snooping fc-map on a VLAN:

```
(config)# vlan 10
(config-vlan)# fip-snooping enable
(config-vlan)# fip-snooping fc-map 0x0efc00
(config-vlan)#
```

Related Commands

Command	Description
fip-snooping enable	Enables FIP snooping on a VLAN.
debug fip-snooping	Debugs a FIP-snooping-enabled module.
show fip-snooping fcf	Displays information about the FIP-snooping Fibre Channel Forwarder (FCF).

Send feedback to nexus4K-docfeedback@cisco.com

fip-snooping port-mode fcf

To configure a Fibre Channel Forwarder (FCF) interface on a bridge, use the **fip-snooping port-mode fcf** command. To remove the configuration, use the **no** form of this command.

fip-snooping port-mode fcf

no fip-snooping port-mode fcf

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable FIP snooping on the switch by using the **feature fip-snooping** command. The commands for configuring FIP snooping are not visible until you enable this feature.

Examples

This example shows how to configure a Fibre Channel Forwarder (FCF) interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# fip-snooping port-mode fcf
switch(config-if)#
```

Related Commands

Command	Description
feature fip-snooping	Enables FIP snooping on the switch.
show fip-snooping fcf	Displays information about the FIP-snooping Fibre Channel Forwarder (FCF).

Send feedback to nexus4K-docfeedback@cisco.com

interface

To configure an interface in order for relaying the FIP packets, use the **interface** command.

interface ethernet *slot*

Syntax Description

ethernet	Specifies an Ethernet module.
slot	Ethernet interface slot number and port number specified in the format 1/1.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to configure an Ethernet interface to relay the FIP packets:

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

Related Commands

Command	Description
fip-snooping port-mode fcf	Configures a FIP-snooping Fibre Channel Forwarder (FCF) interface.

Send feedback to nexus4K-docfeedback@cisco.com

lldp

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp** command. To disable LLDP on an interface, use the **no** form of this command.

lldp {**receive** | **transmit**}

no lldp {**receive** | **transmit**}

Syntax Description

receive	Enables an interface to receive LLDP transmissions.
transmit	Enables LLDP transmission on an interface.

Command Default

Enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable LLDP transmission on the interface Ethernet 1/1:

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

Related Commands

Command	Description
show lldp	Displays LLDP information.

Send feedback to nexus4K-docfeedback@cisco.com

priority-flow-control mode

To configure the priority flow control (PFC) mode on an interface, use the **priority-flow-control mode** command.

priority-flow-control mode {**auto** | **on**}

Syntax Description

auto	Sets the PFC mode to automatic.
on	Forcefully sets the PFC mode to ON.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to configure the PFC mode on an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# priority-flow-control mode auto
switch(config-if)#
```

Related Commands

Command	Description
show interface priority-flow-control	Displays the PFC details for a specified interface.

Send feedback to nexus4K-docfeedback@cisco.com

service-policy (system)

To apply a policy map to the system, use the **service-policy** command. To remove a policy map from the system, use the **no** form of this command.

service-policy type {**network-qos** {*policy-map-name* | **p-nq-5e** | **p-nq-6e** | **p-nq-8e**} | **queuing output** *policy-map-name*}

no service-policy type {**network-qos** {*policy-map-name* | **p-nq-5e** | **p-nq-6e** | **p-nq-8e**} | **queuing output** *policy-map-name*}

Syntax Description

type	Specifies the type of this policy-map.
network-qos	Specifies a policy map of type network qos.
queuing	Specifies a policy map of type queuing.
output	Applies the policy map to packets going out of the interfaces.
p-nq-5e	Specifies a 5 Ethernet policy template.
p-nq-6e	Specifies a 6 Ethernet policy template.
p-nq-8e	Specifies a 8 Ethernet policy template.
policy-map-name	Name of the policy map to apply to all the interfaces in the system. The name can be maximum 40 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must configure quality of service (QoS) policy maps of type queuing or network-qos. A policy can be configured with no-drop, bandwidth, and maximum transmission unit (MTU) configuration, and applied to all interfaces in the system.

Examples

This example shows how to configure a system policy and view the system-wide policies:

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type network-qos my_policy1
switch(config-sys-qos)# show running-config ipqos
version 4.1(2)E1(1)
policy-map type network-qos my_policy1
  class type network-qos c-nq-5e-ndrop
    pause no-drop
    mtu 2500
system qos
  service-policy type queuing output default-out-policy
```

Send feedback to nexus4K-docfeedback@cisco.com

```
  service-policy type network-qos my_policy1

switch(config-sys-qos)#
```

Related Commands

Command	Description
show running-config ipqos	Displays information about the running-system configuration for quality of service (QoS).
system qos	Configures system policies.

Send feedback to nexus4K-docfeedback@cisco.com

show fip-snooping enode

To display information about a FIP-snooping enode, use the **show fip-snooping enode** command.

show fip-snooping enode

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

FIP-snooping must be enabled on the switch.

Examples

The following is sample output from the **show fip-snooping enode** command and displays information about a FIP-snooping enode:

```
switht# show fip-snooping enode

  Legend:
--------------------------------------------------------------------------------
Interface   VLAN     Name ID        FIP MAC           FCID

--------------------------------------------------------------------------------
Eth1/7      1       00000000   00:0c:29:65:82:bc    0x000000

switch#
```

Related Commands

Command	Description
show fip-snooping fcf	Displays information about the FIP-snooping Fibre Channel Forwarder (FCF).

Send feedback to nexus4K-docfeedback@cisco.com

show fip-snooping fcf

To display information about the FIP-snooping Fibre Channel Forwarder (FCF), use the **show fip-snooping fcf** command.

show fip-snooping fcf

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

FIP-snooping must be enabled on the switch.

Examples

The following is sample output from the **show fip-snooping fcf** command and displays information about a FIP-snooping FCF:

```
switch# show fip-snooping fcf
Legend:
------------------------------------------------------------------------------
Interface VLAN No of  FPMA/ FCMAP      FCF-MAC          NameID    Fabric Name
              Enodes SPMA
------------------------------------------------------------------------------
Eth1/1    101  0      FPMA 0x0efc00 00:0d:ec:b1:9e:80 20:65:00:0d: 20:65:00:0d:
                                                      ec:b1:9e:81  ec:97:52:c1
switch#
```

Related Commands

Command	Description
show fip-snooping enode	Displays information about the FIP-snooping enode.

Send feedback to nexus4K-docfeedback@cisco.com

show fip-snooping sessions

To display information about the FIP-snooping sessions, use the **show fip-snooping sessions** command.

show fip-snooping sessions

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

FIP-snooping must be enabled on the switch.

Examples

The following is sample output from the **show fip-snooping sessions** command and displays information about the FIP-snooping sessions:

```
switch# show fip-snooping sessions

  Legend:
--------------------------------------------------------------------------------
 FCF MAC               ENode MAC       VLAN      FCoE MAC         N_PORT_ID

--------------------------------------------------------------------------------
00:0d:ec:b1:9e:80    00:0c:29:71:b5:cb  101     0e:fc:00:5a:00:01  5a:00:01

switch#
```

Related Commands

Command	Description
show fip-snooping enode	Displays information about the FIP-snooping enode.
show fip-snooping fcf	Displays information about the FIP-snooping FCoE Forwarder (FCF).

Send feedback to nexus4K-docfeedback@cisco.com

show lldp

To display the Link Level Discovery Protocol (LLDP) parameters configured on an interface, use the **show lldp** command.

show lldp {[**traffic**] **interface ethernet** *slot* | **neighbors** | **timers**}

Syntax Description

interface	Displays LLDP information for an interface.
ethernet	Specifies the Ethernet interface.
slot	Ethernet interface slot number and port number specified in the format 1/1.
neighbors	Displays LLDP neighbors.
timers	Displays the LLDP timers configured on an interface.
traffic	Displays the LLDP counters configured on an interface.

Command Default

No default behavior or values.

Command Modes

EXEC

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show lldp interface** command and displays LLDP information about an Ethernet interface:

```
switch# show lldp interface ethernet 1/1
tx_enabled: TRUE
rx_enabled: TRUE
dcbx_enabled: TRUE


Port MAC address:  00:05:ad:00:35:60

Remote Peers Information

No remote peers exist
switch#
```

The following is sample output from the **show lldp neighbors** command and displays the LLDP neighbors:

```
switch# show lldp neighbors
LLDP Neighbors

Remote Peers Information on interface Eth1/19
Remote peer's MSAP: length 12 Bytes:
00    0d    ec    a4    2f    80    00    0d    ec    a4    2f    8c
```

Send feedback to nexus4K-docfeedback@cisco.com

```
LLDP TLV's
LLDP TLV type:Chassis ID  LLDP TLV Length: 7
LLDP TLV type:Port ID  LLDP TLV Length: 7
LLDP TLV type:Time to Live  LLDP TLV Length: 2
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 82
LLDP TLV type:END of LLDPDU  LLDP TLV Length: 0

switch#
```

The following is sample output from the **show lldp timers** command and displays the LLDP timers:

```
switch# show lldp timers
LLDP Timers

holdtime 120 seconds
reinit 2 seconds
msg_tx_interval 30 seconds

switch#
```

The following is sample output from the **show lldp traffic** command and displays the LLDP counters on an interface:

```
switch# show lldp traffic interface ethernet 1/1
LLDP traffic statistics:

    Total frames out: 217
    Total Entries aged: 0
    Total frames in: 0
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0

switch#
```

Related Commands

Command	Description
lldp	Configures Link Level Discovery Protocol (LLDP).
show interface ethernet	Displays status and configuration information about Ethernet interfaces.

Send feedback to nexus4K-docfeedback@cisco.com

show policy-map type network-qos

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

show policy-map type network-qos [*policy-map-name*]

Syntax Description

policy-map-name	(Optional) Name of a policy map. The name can be maximum 40 characters.

Command Default

Displays all network-qos policy maps configured in the system.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify a network-qos policy map name, the system displays all the network-qos policy maps.

Examples

The following is sample output from the **show policy-map type network-qos** command and displays information about the network-qos policy maps in the system:

```
switch# show policy-map type network-qos

  Type network-qos policy-maps
  ============================

    policy-map type network-qos p-nq-5e
        class-map  c-nq-5e-drop
        pause
        class-map  c-nq-5e-ndrop
        pause no-drop
        mtu 2112

    policy-map type network-qos p-nq-6e
        class-map  c-nq-6e-drop
        pause

        class-map  c-nq-6e-ndrop
        pause no-drop
        mtu 2112

    policy-map type network-qos p-nq-8e
        class-map  c-nq-8e
        pause

    policy-map type network-qos policy-fcoe
        class-map  class-fcoe
        pause no-drop
```

Send feedback to nexus4K-docfeedback@cisco.com

```
        mtu 2500

        class-map  class-non-fcoe

    policy-map type network-qos my_policy1
        class-map  c-nq-5e-ndrop
        pause no-drop
        mtu 2500

switch#
```

Related Commands

Command	Description
show policy-map type queuing	Displays the queuing policy maps.

Send feedback to nexus4K-docfeedback@cisco.com

show policy-map type queuing

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

show policy-map type queuing [*policy-map-name*]

Syntax Description

policy-map-name	(Optional) Name of a policy map. The name can be maximum 40 characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If you do not specify a policy map name, the system displays all the queuing policy maps.

Examples

The following is sample output from the **show policy-map type queuing** command and displays information about the queuing policy maps in the system:

```
switch# show policy-map type queuing

Type queuing policy-maps
  ========================

  policy-map type queuing default-out-policy
    class type queuing out-pq1
    class type queuing out-q2
    class type queuing out-q3
    class type queuing out-q-default

policy-map type queuing policy-fcoe-bandwidth
    class type queuing 1p7q4t-out-q-default
      bandwidth percent 50
switch#
```

Related Commands

Command	Description
show policy-map type network-qos	Displays the network-qos policy maps.

Send feedback to nexus4K-docfeedback@cisco.com

switchport mode trunk

To configure an Ethernet interface as a trunk port, use the **switchport mode trunk** command. To remove the configuration, use the **no** form of this command.

switchport mode trunk

no switchport mode trunk

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The Ethernet interface must be configured as a trunk port to allow both Fibre Channel and Ethernet traffic on the same interface.

Examples

This example shows how to enable the trunk mode for the interface Ethernet 1/1:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode trunk
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays switch port information of interfaces.

Send feedback to nexus4K-docfeedback@cisco.com

switchport trunk allowed vlan

To configure the VLANs that are allowed on a trunk interface, use the **switchport trunk allowed vlan** command. To remove the configuration, use the **no** form of this command.

switchport trunk allowed vlan {[**add** | **except** | **remove**] *vlan-id* | **all** | **none**}

no switchport trunk allowed vlan {[**add** | **except** | **remove**] *vlan-id* | **all** | **none**}

Syntax Description

vlan-id	Specifies a single VLAN ID or a range of VLAN IDs. For example, 1, 30-50, 60-90.
add	(Optional) Adds VLANs to the current list of allowed VLANs.
all	Specifies all VLANs to be configured for trunking.
except	(Optional) Specifies that all VLANs, except the specified VLANs in the allowed list, will be configured for trunking.
none	Specifies that no VLANs in the allowed list will be configured for trunking.
remove	(Optional) Removes specified VLANs from the list of allowed VLANs.

Command Default

The default is to allow all VLANs on the trunk interface, from 1 to 3967 and 4048 to 4094.

By default, all VLANs are allowed on all trunk interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you configure the allowed VLANs for the specified trunk ports, ensure that you are configuring the correct interfaces and that the interfaces are trunks.

Examples

This example shows how to configure a VLAN as the allowed list of VLANs for an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport trunk allowed vlan 100
switch(config-if)#
```

This example shows how to configure a range of VLANs as the allowed list of VLANs for an interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport trunk allowed vlan 1,30-50,60-90
switch(config-if)#
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
show interface switchport	Displays switch port information of interfaces.

Send feedback to nexus4K-docfeedback@cisco.com



CHAPTER 7

System Management Commands

This chapter describes the system management commands available on the switch.

Send feedback to nexus4K-docfeedback@cisco.com

clear logging nvram

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

clear logging nvram

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear the NVRAM logs:

```
switch# clear logging nvram
```

Related Commands

Command	Description
show logging nvram	Displays the NVRAM logs.

Send feedback to nexus4K-docfeedback@cisco.com

clear logging onboard

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

clear logging onboard [**environmental-history** | **exception-log** | **obfl-logs** | **system-health**]

Syntax Description

environmental-history	(Optional) Clears the OBFL environmental history.
exception-log	(Optional) Clears the OBFL exception log entries.
obfl-logs	(Optional) Clears the OBFL entries for boot-uptime, device version, and OBFL history.
system-health	(Optional) Clears the OBFL system health entries.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

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

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

The following example shows how to clear the OBFL entries for boot-uptime, device version, and OBFL history:

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

The following example shows how to clear the OBFL system health entries:

```
switch# clear logging onboard system-health
```

Related Commands

Command	Description
show logging onboard	Displays onboard failure logs.

Send feedback to nexus4K-docfeedback@cisco.com

clear ntp statistics

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

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

Syntax Description

all-peers	Clears all peer or server association statistics.
io	Clears I/O statistics.
local	Clears local statistics.
memory	Clears memory statistics.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
show ntp peers	Displays the configured server and peer associations.
show ntp statistics	Displays NTP statistics.

Send feedback to nexus4K-docfeedback@cisco.com

logging console

To enable the switch to log messages to the console session based on a specified severity level or higher, use the **logging console** command. To disable the switch from logging messages to the console, use the **no** form of this command.

logging console [*severity-level*]

no logging console [*severity-level*]

Syntax Description

severity-level	(Optional) Specifies the minimum severity level at which messages are logged. If the severity level is not specified, the default of 2 is used.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.

When you configure the severity level, the system outputs messages at that level and lower. Table 7-1 describes the severity levels used in system messages.

Table 7-1 System Message Severity Levels

Level	Description
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

Send feedback to nexus4K-docfeedback@cisco.com

Examples

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

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging console	Displays the console logging configuration.
show logging nvram	Displays the system messages in the NVRAM log.

Send feedback to nexus4K-docfeedback@cisco.com

logging event

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

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

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

Syntax Description

link-status	Log all UP/DOWN and CHANGE messages.
trunk-status	Log all TRUNK status messages.
default	The default logging configuration is used by interfaces not explicitly configured.
enable	To enable logging overriding port level configuration.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to log interface events:

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging info	Displays the logging configuration.

Send feedback to nexus4K-docfeedback@cisco.com

logging event port

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

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

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

Syntax Description

link-status	Log all UP/DOWN and CHANGE messages.
trunk-status	Log all TRUNK status messages.
default	(Optional) The default logging configuration is used by interfaces not explicitly configured.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to log interface events on Ethernet 1/1:

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show interface	Displays the interface configuration information.
show logging info	Displays the logging configuration.

Send feedback to nexus4K-docfeedback@cisco.com

logging level

To enable the switch to log messages from a facility based on a specified severity level or higher, use the **logging level** command. To disable the switch from 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	Specifies the appropriate facility. Table 7-2 lists the facilities available in the switch.
severity-level	Specifies the minimum severity level at which messages are logged. Table 7-1 lists the severity levels used in system messages.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

To apply the same severity level to all facilities, use the **all** facility. To view the default severity levels assigned to each facility, use the **show logging level** command.

Examples

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

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging level	Displays the facility logging level configuration.

Send feedback to nexus4K-docfeedback@cisco.com

logging logfile

To configure the switch to log system messages to a file, use the **logging logfile** command. To disable the switch from logging system messages to a file, use the **no** form of this command.

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

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

Syntax Description

logfile-name	Name of the log file to be used to store system messages.
severity-level	Specifies the minimum severity level at which messages are logged. The default severity level is 5. Table 7-1 describes the severity levels used in system messages.
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

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to configure a log file called *my_logsl4* to store system messages with severity level 4:

```
switch(config)# logging logfile my_logsl4 4
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging info	Displays the logging configuration.
show logging logfile	Displays the log file.

Send feedback to nexus4K-docfeedback@cisco.com

logging module

To configure the severity level and time-stamp units of messages logged by modules, use the **logging module** command. To disable module log messages, use the **no** form of this command.

logging module [*severity-level*]

no logging module

Syntax Description

severity-level	(Optional) Specifies the minimum severity level at which messages are logged. Table 7-1 describes the severity levels used in system messages.

Command Default

Severity level 5 (notifications) messages are logged.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable module log messages:

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging module	Displays the module logging configuration.

Send feedback to nexus4K-docfeedback@cisco.com

logging monitor

To enable the switch to log messages to the monitor (terminal line) based on a specified severity level or higher, use the **logging monitor** command. This configuration applies to Telnet and SSH sessions. To disable logging messages to Telnet and SSH sessions, use the **no** form of this command.

logging monitor [*severity-level*]

no logging monitor [*severity-level*]

Syntax Description

severity-level	(Optional) Specifies the minimum severity level at which messages are logged. Table 7-1 describes the severity levels used in system messages.

Command Default

Enabled (severity: notification).

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If the severity level is not specified, the default of 5 (notification) is used.

Examples

This example shows how to enable monitor log messages to the default severity level 5 (notification):

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging monitor	Displays the monitor logging configuration.

Send feedback to nexus4K-docfeedback@cisco.com

logging server

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

logging server *host* [*severity-level*] [**facility** *facility*]

no logging server *host*

Syntax Description

host	Configures the hostname or IPv4 address of the Remote Syslog Server.
severity-level	(Optional) Specifies the minimum severity level at which messages are logged. Table 7-1 lists the severity levels used in system messages.
facility *facility*	(Optional) Specifies the outgoing facility. The default outgoing facility is **local7**.

Command Default

The default outgoing facility is **local7**.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can use the auth, authpriv, cron, daemon, ftp, kernel, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, news, syslog, user, and uucp facilities to configure a syslog server. Table 7-2 describes the facilities.

Examples

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

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

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

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging server	Displays the configured syslog servers.

Send feedback to nexus4K-docfeedback@cisco.com

logging timestamp

To set the logging timestamp units, use the **logging timestamp** command. 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

Timestamp unit is **seconds**.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show logging timestamp	Displays the logging timestamp configuration.

Send feedback to nexus4K-docfeedback@cisco.com

ntp

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

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure NTP using either IPv4 addresses or Domain Name System (DNS) names.

You can have multiple peer or server associations.

Examples

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

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

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

```
switch(config)# ntp peer 192.168.2.168
```

This example deletes an association with a peer:

```
switch(config)# no ntp peer 192.168.2.168
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show ntp peers	Displays the configured server and peer associations.

Send feedback to nexus4K-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

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show ntp peers	Displays the configured server and peer associations.

Send feedback to nexus4K-docfeedback@cisco.com

show logging console

To display the console logging configuration, use the **show logging console** command.

show logging console

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging console** command and displays information about the console logging configuration:

```
switch# show logging console
Logging console:                enabled (Severity: critical)
switch#
```

Related Commands

Command	Description
logging console	Configures logging to the console.

Send feedback to nexus4K-docfeedback@cisco.com

show logging info

To display the logging configuration, use the **show logging info** command.

show logging info

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging info** command and displays information about the logging configuration in a switch:

```
switch# show logging info

Logging console:                disabled
Logging monitor:                enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - messages: Severity - notifications Size - 10485760

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclmgr                  3                       3
aclqos                  5                       5
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
clis                    7                       7
confcheck               2                       2
cron                    3                       3
daemon                  3                       3
dcbx                    2                       2
eth_port_channel        5                       5
ethpc                   2                       2
ethpm                   5                       5
evmc                    5                       5
feature-mgr             2                       2
ftp                     3                       3
fwm                     6                       6
```

Send feedback to nexus4K-docfeedback@cisco.com

```
ifmgr                 5                   5
igmp_1                5                   4
ip                    3                   3
ipqosmgr              4                   4
ipv6                  3                   3
kern                  3                   3
l3vm                  5                   5
licmgr                6                   6
local0                3                   3
local1                3                   3
local2                3                   3
local3                3                   3
local4                3                   3
local5                3                   3
local6                3                   3
local7                3                   3
lpr                   3                   3
mail                  3                   3
monitor               3                   3
mvsh                  2                   2
news                  3                   3
ntp                   2                   2
platform              5                   5
radius                3                   3
res_mgr               5                   5
securityd             3                   3
solm                  2                   2
stp                   3                   3
syslog                3                   3
sysmgr                3                   3
SystemHealth          4                   4
u6rib                 5                   5
urib                  5                   5
user                  3                   3
uucp                  3                   3
vdc_mgr               6                   6
vlan_mgr              2                   2
vshd                  5                   5
xmlma                 3                   3

0(emergencies)        1(alerts)       2(critical)
3(errors)             4(warnings)     5(notifications)
6(information)        7(debugging)

switch#
```

Related Commands

Command	Description
logging event	Configures logging interface events.
logging event port	Configures logging of events for a specific interface.
logging logfile	Configures the switch to log system messages to a file.

Send feedback to nexus4K-docfeedback@cisco.com

show logging last

To display the last number of lines of the logfile, use the **show logging last** command.

show logging last *number*

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

Command Default No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples The following is sample output from the **show logging last 5** command and displays the last 5 lines of the log file:

```
switch-nx4# show logging last 5
2009 Aug 12 05:50:42 switch-nx4 %ETHPORT-5-SPEED: Interface Ethernet1/16,
 operational speed changed to 10 Gbps
2009 Aug 12 05:50:42 switch-nx4 %ETHPORT-5-IF_DUPLEX: Interface Ethernet1
/16, operational duplex mode changed to Full
2009 Aug 12 05:50:42 switch-nx4 %ETHPORT-5-IF_RX_FLOW_CONTROL: Interface
Ethernet1/16, operational Receive Flow Control state changed to off
2009 Aug 12 05:50:42 switch-nx4 %ETHPORT-5-IF_TX_FLOW_CONTROL: Interface
Ethernet1/16, operational Transmit Flow Control state changed to off
2009 Aug 12 05:50:42 switch-nx4 %ETHPORT-5-IF_UP: Interface Ethernet1/16
is up in mode access
switch-nx4#
```

Related Commands	Command	Description
	show logging logfile	Displays the logging information in a log file.

Send feedback to nexus4K-docfeedback@cisco.com

show logging level

To display the facility logging severity level configuration, use the **show logging level** command.

show logging level [*facility*]

Syntax Description

facility	(Optional) Specifies the logging facility. Table 7-2 lists the facilities available in the switch.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging level port-channel** command and displays information about the EtherChannel logging severity level configuration:

```
switch# show logging level port-channel
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
eth_port_channel        5                       5

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

switch#
```

Related Commands

Command	Description
logging level	Configures the facility logging level.

Send feedback to nexus4K-docfeedback@cisco.com

show logging logfile

To display the messages in the log file that have a time stamp within the span entered, use the **show logging logfile** command. 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) Specifies the start time in the format *yyyy mmm dd hh:mm:ss*.
end-time	(Optional) Specifies the end time in the format *yyyy mmm dd hh:mm:ss*.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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.

Examples

The following is sample output from the **show logging logfile** command and displays the messages in the log file that were timestamped within the span shown:

```
switch# show logging logfile start-time 2009 aug 12 03:56:29 end-time 2009 aug 12 03:56:31
2009 Aug 12 03:56:29  %PFMA-5-PFM_NOPROTECTED_MODE_TAKES_EFFECT: Disabled Protec
ted Mode takes effect.
2009 Aug 12 03:56:31  %KERN-2-SYSTEM_MSG: Starting kernel... - kernel
2009 Aug 12 03:56:31  %KERN-1-SYSTEM_MSG:  Entered kgdb_console_init:1960 - kern
el
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: ohci_hcd 0001:03:14.0: Found HC with n
o IRQ.  Check BIOS/PCI 0001:03:14.0 setup! - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: cctrlCard Mode = 1 - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: sda: assuming drive cache: write throu
gh - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: sda: assuming drive cache: write throu
gh - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: ismic init_module: diag card type chec
k failed: 6<3>psoc init_module: diag card type check failed: 6<3>CMOS: Module in
itialized - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: 802.1Q VLAN Support v1.8 Ben Greear <g
reearb@candelatech.com> - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: All bugs added by David S. Miller <dav
em@redhat.com> - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: 1 Initializing the kernel module
- kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: 2 Initializing the kernel module
- kernel
```

Send feedback to nexus4K-docfeedback@cisco.com

```
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: 3 Initializing the kernel module
- kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: 4 Initializing the kernel module
- kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: 5 Initializing the kernel module
- kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: 6 Initializing the platform speci
fic module - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: pfm_taishan_driver_toggle_wdt dis
abled - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: pfm_taishan_driver_toggle_wdt ena
bled - kernel
2009 Aug 12 03:56:31  %KERN-3-SYSTEM_MSG: PFM: pfm_taishan_driver_set_wdt_brkpt
is_enable:0x1 - kernel

switch#
```

Related Commands

Command	Description
logging logfile	Configures logging to a log file.

Send feedback to nexus4K-docfeedback@cisco.com

show logging module

To display the module logging configuration, use the **show logging module** command.

show logging module

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging module** command and displays information about the module logging configuration:

```
switch# show logging module
Logging linecard:                enabled (Severity: notifications)
switch#
```

Related Commands

Command	Description
logging module	Configures module logging.

Send feedback to nexus4K-docfeedback@cisco.com

show logging monitor

To display the monitor logging configuration, use the **show logging monitor** command.

show logging monitor

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging monitor** command and displays information about the monitor logging configuration:

```
switch# show logging monitor
Logging monitor:                enabled (Severity: notifications)
switch#
```

Related Commands

Command	Description
logging monitor	Configures system message logging on the monitor.

Send feedback to nexus4K-docfeedback@cisco.com

show logging nvram

To display the messages in the NVRAM log, use the **show logging nvram** command.

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

Syntax Description

last *number-lines*	(Optional) Specifies the last number of lines to display from the NVRAM log. Valid values range from 1 to 100 lines.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.

Examples

The following is sample output from the **show logging nvram last 3** command and displays the last 3 messages in the NVRAM log:

```
switch-nx4# show logging nvram last 3
2009 Aug 11 09:28:02 switch-nx4 %PFMA-2-MOD_TEMPMINALRM: sup reported min
or temperature alarm. Sensor=4 Temperature=54 MinThreshold=50
2009 Aug 11 09:27:28 switch-nx4 %VDC_MGR-2-VDC_ONLINE: vdc 1 has come onl
ine
2009 Aug 11 09:26:59 switch-nx4 %KERN-1-SYSTEM_MSG:  Entered kgdb_console
_init:1960 - kernel
switch-nx4#
```

Related Commands

Command	Description
logging console	Configures system message logging to the console.

Send feedback to nexus4K-docfeedback@cisco.com

show logging onboard

To display the onboard failure logging (OBFL) information, use the **show logging onboard** command.

show logging onboard {**boot-uptime** | **device-version** | **endtime** | **environmental-history** | **exception-log** | **obfl-history** | **obfl-logs** | **starttime** | **status** | **system-health**} [> *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.
obfl-history	Displays the following OBFL history information: • Timestamp when OBFL was manually disabled. • Timestamp when OBFL was manually enabled. • Timestamp when OBFL data was manually cleared.
obfl-logs	Displays the OBFL technical support log 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.
system-health	Displays the OBFL system health information.
> *file*	(Optional) Redirects the output to a file. See the “Usage Guidelines” section for additional information.
| *type*	(Optional) Filters the output. Table 1-8 lists the valid values for filter *type*.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

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.

Send feedback to nexus4K-docfeedback@cisco.com

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.

Specifying Start Date and End Time

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

Redirecting Output to a File

The output from the show configuration session command is very long. To better manage this output, you can redirect the output to a file (for example, **show logging onboard boot-uptime** > *filename*) in the local writable storage file system or the remote file system.

The syntax for the filename string is as follows:

filesystem://*server*/*directory*/*filename*

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

Use the URL prefix keywords for local writable storage file systems or remote file systems. 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. For remote file systems, if it is not otherwise specified, the path is the default for the user on the remote server.

Examples

The following is sample output from the **show logging onboard status** command and displays information about the status of the OBFL:

```
switch# show logging onboard status
----------------------------
OBFL Status
----------------------------
    Switch OBFL Log:                                    Enabled

    Module:  1 OBFL Log:                                Enabled
    environmental-history                               Enabled
    exception-log                                       Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    temp error                                          Enabled
    stack-trace                                         Enabled
switch#
```

The following is sample output from the **show logging onboard boot-uptime** command and displays information about the OBFL boot and uptime:

```
switch# show logging onboard boot-uptime

Wed Aug 12 05:28:25 2009:  Boot Record
------------------------------------------------------------
Boot Time..........:  Wed Aug 12 05:28:25 2009
Slot Number........:  1
Serial Number......:  JAB1251003C
```

Send feedback to nexus4K-docfeedback@cisco.com

```
Bios Version.......:    v1.0.31(08/05/09)
Firmware Version...:  4.1(2)E1(1) [build 4.1(2)E1(0.157)]


Wed Aug 12 05:34:56 2009:  Boot Record
------------------------------------------------------------
Boot Time..........:  Wed Aug 12 05:34:56 2009
Slot Number........:  1
Serial Number......:  JAB1251003C
Bios Version.......:    v1.0.31(08/05/09)
Firmware Version...:  4.1(2)E1(1) [build 4.1(2)E1(0.157)]

Wed Aug 12 05:28:33 2009:  Card Uptime Record
---------------------------------------------
Uptime: 84, 0 days 0 hour(s) 1 minute(s) 24 second(s)
Reset Reason: Unknown (0)
Reset Reason SW: Reset triggered due to HA policy of Reset (16)
Reset Reason HW: Unknown (0)
Card Mode..........................:  Runtime



Wed Aug 12 05:35:04 2009:  Card Uptime Record
---------------------------------------------
Uptime: 78, 0 days 0 hour(s) 1 minute(s) 18 second(s)
Reset Reason: Unknown (0)
Reset Reason SW: Reset Requested by CLI command reload (9)
Reset Reason HW: Unknown (0)
Card Mode..........................:  Runtime

switch#
```

The following is sample output from the **show logging onboard device-version** command and displays information about the OBFL logging device information:

```
switch# show logging onboard device-version
----------------------------
OBFL Data for
    Module:  1
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                 Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Tue Aug 11 00:57:52 2009   ELECTRA                0        1        1
Tue Aug 11 01:28:46 2009   ELECTRA                0        1        1
Tue Aug 11 03:11:58 2009   ELECTRA                0        1        1
Tue Aug 11 04:51:21 2009   ELECTRA                0        1        1
Tue Aug 11 05:08:00 2009   ELECTRA                0        1        1
Tue Aug 11 05:18:16 2009   ELECTRA                0        1        1
Tue Aug 11 09:27:35 2009   ELECTRA                0        1        1
Tue Aug 11 09:42:35 2009   ELECTRA                0        1        1
Tue Aug 11 13:26:58 2009   ELECTRA                0        1        1
Tue Aug 11 14:03:34 2009   ELECTRA                0        1        1
Tue Aug 11 14:23:33 2009   ELECTRA                0        1        1
Tue Aug 11 21:41:49 2009   ELECTRA                0        1        1
Tue Aug 11 22:48:59 2009   ELECTRA                0        1        1
Tue Aug 11 22:54:46 2009   ELECTRA                0        1        1
Tue Aug 11 22:59:18 2009   ELECTRA                0        1        1
Wed Aug 12 00:41:21 2009   ELECTRA                0        1        1
Wed Aug 12 03:57:05 2009   ELECTRA                0        1        1
Wed Aug 12 05:28:33 2009   ELECTRA                0        1        1
```

Send feedback to nexus4K-docfeedback@cisco.com

```
Wed Aug 12 05:35:04 2009   ELECTRA                0        1        1
switch#
```

The following is sample output from the **show logging onboard obfl-history** command and displays information about the OBFL history information:

```
switch# show logging onboard obfl-history
```

Related Commands

clear logging onboard	Clears the OBFL entries in the persistent log.

Send feedback to nexus4K-docfeedback@cisco.com

show logging server

To display the syslog server configuration, use the **show logging server** command.

show logging server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging server** command and displays information about the syslog server configuration:

```
switch# show logging server
Logging server:                 disabled
switch#
```

Related Commands

Command	Description
logging server	Configures a remote syslog server.

Send feedback to nexus4K-docfeedback@cisco.com

show logging timestamp

To display the logging timestamp configuration, use the **show logging timestamp** command.

show logging timestamp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show logging timestamp** command and displays information about the logging timestamp configuration:

```
switch# show logging timestamp
Logging timestamp:              Seconds
switch#
```

Related Commands

Command	Description
logging timestamp	Configures the logging timestamp granularity.

Send feedback to nexus4K-docfeedback@cisco.com

show ntp peers

To display information about Network Time Protocol (NTP) peer and server associations, use the **show ntp peers** command.

show ntp peers

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show ntp peers** command and displays information about the NTP peers:

```
switch# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  192.168.2.16                  Server (configured)
switch#
```

Related Commands

Command	Description
ntp	Configures NTP peers.

Send feedback to nexus4K-docfeedback@cisco.com

show ntp statistics

To display Network Time Protocol (NTP) statistics, use the **show ntp statistics** command.

show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** *address* | **name** *name1* [**..***nameN*]}

Syntax Description

io	Show the input-output statistics.
local	Show the counters maintained by the local NTP.
memory	Show the statistics counters related to memory code.
peer	Show the per-peer statistics counter of a peer.
ipaddr *address*	Displays statistics for the peer with the configured IPv4 address. The IPv4 address format is dotted decimal, x.x.x.x.
name *name1* [*..nameN*]	Displays statistics for one or more named peers.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show ntp statistics local** command and displays the statistics for NTP:

```
switch(config)# show ntp statistics local
system uptime:          2042
time since reset:       2042
old version packets:    272
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      272
bad authentication:     0
switch#
```

The following is sample output from the **show ntp statistics peer** command and displays the statistics for an NTP peer:

```
switch(config)# show ntp statistics peer ipaddr 192.168.2.1
remote host:          192.168.2.1
local interface:      Unresolved
time last received:   9s
time until next send: 40s
reachability change:  1211s
packets sent:         222
packets received:     221
bad authentication:   0
bogus origin:         0
```

Send feedback to nexus4K-docfeedback@cisco.com

```
duplicate:            0
bad dispersion:       0
bad reference time:   0
candidate order:      6
switch#
```

The following is sample output from the **show ntp statistics memory** command and displays information about the statistics counters related to memory code for the NTP:

```
switch(config)# show ntp statistics memory
time since reset:     2076
total peer memory:    15
free peer memory:     14
calls to findpeer:    280
new peer allocations: 0
peer demobilizations: 0
hash table counts:      0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        1   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
switch#
```

Related Commands

Command	Description
clear ntp statistics	Clears NTP statistics.
ntp	Configures NTP peers.

Send feedback to nexus4K-docfeedback@cisco.com

show vrf

To display virtual routing and forwarding (VRF), use the **show vrf** command.

show vrf [**all** | **management**]

Syntax Description

all	Displays VRF information for all VRFs.
management	Displays VRF management context information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show vrf** command and displays information about the VRF:

```
switch# show vrf
VRF-Name                       VRF-ID    State   Reason
chassis-management                  3    Up      --
default                             1    Up      --
management                          2    Up      --
switch#
```

The following is sample output from the **show vrf management** command and displays the VRF information for management interfaces:

```
switch# show vrf management
VRF-Name                       VRF-ID    State   Reason
management                          2    Up      --
switch#
```

Related Commands

Command	Description
use-vrf	Specifies a VRF instance for a RADIUS or TACACS+ server group.
vrf context	Configures a VRF instance.

Send feedback to nexus4K-docfeedback@cisco.com

System Message Logging Facilities

Table 7-2 lists the facilities that you can use in system message logging configuration.

Table 7-2 System Message Logging Facilities

Facility	Description
aaa	Sets level for aaa syslog messages.
adjmgr	Sets syslog filter level for Adjacency Manager.
all	Sets level for all facilities.
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.
cdp	Sets logging level for CDP.
cron	Sets level for Cron/at facility.
daemon	Sets level for System daemons.
dcbx	Sets level for dcx syslog messages.
ethpc	Sets level for ethpc syslog messages.
ethpm	Sets level for ethpm syslog messages.
fip-snooping	Sets the Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping syslog level. **Note** This facility appears only if FIP snooping is enabled on the switch.
ftp	Sets level for File Transfer System.
fwm	Sets level for fwm syslog messages.
im	Sets level for im syslog messages.
ipconf	Sets the ipconf logging syslog level.
ipqos	Sets the ipqosmgr logging syslog level.
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.

Send feedback to nexus4K-docfeedback@cisco.com

Table 7-2 System Message Logging Facilities (continued)

Facility	Description
local7	Sets level for Local use daemons.
lpr	Sets level for Line Printer System.
lstsvc	Sets the link-state tracking (LST) logging syslog level.
mail	Sets level for Mail system.
monitor	Sets level for Ethernet span syslog messages.
mvsh	Sets the MVSH manager syslog level.
netstack	Sets the IP net stack syslog level.
news	Sets level for USENET news.
ntp	Sets syslog filter level for NTP.
ohms	Sets the system health syslog level.
port-channel	Sets level for EtherChannel syslog messages.
radius	RADIUS syslog level.
res_mgr	Set slevel for res_mgr syslog messages.
security	Security syslog level.
session-mgr	Sets level for session-manager syslog messages.
snm	Sets the Shared Memory Manager (SNM) syslog level.
snmpd	Sets the SNMP syslog level.
spanning-tree	Sets level for stp syslog messages.
syslog	Sets level for Internal Syslog Messages.
sysmgr	System Manager syslog level.
u6rib	Sets syslog filter level for U6RIB.
udld	Sets syslog filter level for the Cisco-proprietary Unidirectional Link Detection (UDLD) protocol. **Note** This facility appears only if the UDLD feature is enabled on the switch.
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.
vshd	Sets logging level for vshd.
xml	XML agent syslog level.

Send feedback to nexus4K-docfeedback@cisco.com

vrf context

To create a virtual routing and forwarding (VRF) instance and enter vrf context configuration mode, use the **vrf context** command. To remove a VRF entry, use the **no** form of this command.

vrf context {*name* | **management**}

no vrf context {*name* | **management**}

Syntax Description

name	Name of the VRF. The name can be maximum 32 characters.
management	Specifies a configurable VRF name.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When you enter the vrf configuration mode, the following commands are available:

- **exit**—Exits from the current VRF command mode.
- **ip**—Configures IP features.

  Additional commands available in IP configuration mode:
  - **domain-list**—Adds additional domain names.
  - **domain-name**—Specifies the default domain name.
  - **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 the vrf context management configuration mode:

```
switch(config)# vrf context management
switch(config-vrf)#
```

This example shows how to revert to the default VRF IP server:

```
switch(config)# vrf context management
switch(config-vrf)# no ip name-server 192.168.2.1
```

Send feedback to nexus4K-docfeedback@cisco.com

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show vrf	Displays VRF information.



Send feedback to nexus4K-docfeedback@cisco.com

INDEX

A

aaa accounting default command 5-2
aaa authentication login console command 5-4
aaa authentication login default command 5-6
aaa authentication login error-enable command 5-8
aaa authentication login mschap command 5-9
aaa group server radius command 5-10
aaa group server tacacs+ command 5-11
ACL precedence value 5-23
action command 5-12

B

bandwidth (interface) command 2-2
bandwidth (QoS) command 4-2
bandwidth remaining command 4-4
banner motd command 1-2
boot command 1-3

C

cd command 1-5
cdp command 2-4
cdp enable command 2-6
channel-group (Ethernet) command 2-7
cin command 2-10
class map
    queuing default 4-2
    queuing system-defined 4-2
class-map type network-qos command 4-9
class-map type qos command 4-10
class-map type queuing match-any command 4-12
class type network-qos command 4-7
class type qos command 4-5
class type queuing command 4-8
clear access-list counters command 5-13
clear accounting log command 5-14
clear cdp counters command 2-11
clear cdp table command 2-12
clear cli history command 1-6
clear cores command 1-7
clear debug-logfile command 1-8
clear install failure-reason command 1-9
clear license command 1-10
clear logging nvram command 7-2
clear logging onboard command 7-3
clear mac access-list counters command 2-13
clear mac-address-table dynamic command 2-14
clear ntp statistics command 7-4
clear qos statistics command 4-13
clear spanning-tree counters command 2-16
clear spanning-tree detected-protocols command 2-17
clear statistics device all command 4-14
clear user command 1-11
cli alias name command 1-12
cli var name command 1-14
clock set command 1-16
clock summer-time command 1-17
clock timezone command 1-19
configure session command 1-20
configure terminal command 1-21
congestion-control command 4-15
copy command 1-22
copy running-config startup-config command 1-26

Send feedback to nexus4K-docfeedback@cisco.com

D

databits command 1-27
deadtime command 5-15
debug logfile command 1-28
debug logging command 1-29
delay (interface) command 2-18
delete command 1-30
deny (IPv4) command 5-17
deny (MAC) command 5-27
description (interface) command 2-19
description (policy map) command 4-16
description (QoS) command 4-16
description (table map) command 4-16
description (user role) command 5-30
dir command 1-32
DSCP values 5-20

E

echo command 1-34
end command 1-35
exec-timeout command 1-36
exit (EXEC) command 1-38
exit (global) command 1-39

F

feature (role feature-group name) command 5-31
feature fip-snooping command 1-40
feature interface-vlan command 1-41
feature lacp command 1-42
feature lst command 1-43
feature private-vlan command 1-44
feature ssh command 1-45
feature tacacs+ command 1-46
feature telnet command 1-47
feature udld command 1-48
filter types 1-116
find command 1-49
fip-snooping enable command 6-2
fip-snooping fc-map command 6-3
fip-snooping port-mode fcf command 6-4
flowcontrol hardware command 1-50
format command 1-51

G

gunzip command 1-52
gzip command 1-53

H

hostname command 1-54

I

ICMP message types 5-21
install all command 1-55
install license command 1-58
install module bios command 1-57
install module epld command 1-59
instance vlan command 2-20
interface command 6-5
interface ethernet command 2-22
interface policy deny command 5-32
interface port-channel command 2-23
interface vlan command 2-25
ip access-list command 5-33
ip igmp snooping (EXEC) command 2-26
ip igmp snooping (VLAN) command 2-27
ip port access-group command 5-35

L

lacp port-priority command 2-29
lacp system-priority command 2-30

Send feedback to nexus4K-docfeedback@cisco.com

line com1 command 1-60
line console command 1-61
line vty command 1-62
link debounce command 2-31
link state group command 2-32
link state track command 2-34
lldp command 6-6
logging console command 7-5
logging event command 7-7
logging event port command 7-8
logging level command 7-9
logging logfile command 7-10
logging module command 7-11
logging monitor command 7-12
logging server command 7-13
logging timestamp command 7-14

M

mac access-list command 5-37
mac-address-table aging-time command 2-35
mac-address-table notification command 2-37
mac-address-table static command 2-38
mac port access-group command 5-39
match access-group command 4-17
match class-map command 4-18
match command 5-41
match cos command 4-19
modem connect line command 1-63
modem in command 1-64
modem init-string command 1-65
modem restart line command 1-67
modem set-string user-input command 1-68
monitor session command 2-40
move command 1-69
mtu command 4-21

N

name (MST configuration) command 2-42
name (VLAN configuration) command 2-41
ntp command 7-15
ntp sync-retry command 7-16

O

object-group ip address command 5-42
object-group ip port command 5-43

P

parity command 1-71
pause no-drop command 4-22
permit (IPv4) command 5-44
permit (MAC) command 5-49
permit interface command 5-52
permit vlan command 5-54
permit vrf command 5-56
ping command 1-72
platform chassis-management protected-mode command 1-73
policy-map type network-qos command 4-23
policy-map type qos command 4-24
policy-map type queuing command 4-25
port-channel load-balance ethernet command 2-43
priority (queuing) command 4-26
priority-flow-control mode command 6-7
private-vlan association command 2-47
private-vlan command 2-45
private-vlan synchronize command 2-49
pwd command 1-75

Q

qos statistics command 4-28

Send feedback to nexus4K-docfeedback@cisco.com

R

radius-server deadtime command 5-58
radius-server directed-request command 5-59
radius-server host command 5-60
radius-server key command 5-63
radius-server retransmit command 5-65
radius-server timeout command 5-66
reload command 1-76
remark command 5-67
resequence command 5-69
revision command 2-50
rmdir command 1-77
role feature-group name command 5-71
role name command 5-72
rule command 5-74
run-script command 1-78

S

save command 1-79
send command 1-80
server command 5-76
service-policy (interface) command 4-29
service-policy (system) command 6-8
session-limit command 1-82
set cos (policy map type qos) command 4-31
setup command 1-81
shape command 4-32
show aaa accounting command 5-78
show aaa authentication command 5-79
show aaa groups command 5-81
show access-lists command 5-82
show accounting log command 5-83
show banner motd command 1-83
show boot command 1-84
show cdp command 3-2
show chassis summary command 1-85
show class-map type network-qos command 4-34
show class-map type qos command 4-36
show class-map type queuing command 4-37
show cli alias command 1-86
show cli history command 1-87
show cli variables command 1-88
show clock command 1-89
show configuration session command 1-90
show copyright command 1-92
show debug logfile command 1-93
show environment command 1-94
show file command 1-96
show fip-snooping enode command 6-10
show fip-snooping fcf command 6-11
show fip-snooping sessions command 6-12
show hostname command 1-97
show incompatibility system command 1-98
show install all command 1-99
show interface command 3-5
show interface counters storm-control command 5-85
show interface ethernet command 3-6
show interface mac-address command 3-8
show interface port-channel command 3-9
show interface priority-flow-control command 3-11
show interface private-vlan mapping command 3-13
show interface switchport command 3-14
show inventory command 1-100
show ip access-lists command 5-87
show ip igmp snooping command 3-16
show lacp command 3-17
show license command 1-101
show license host-id command 1-102
show license usage command 1-103
show line command 1-105
show link state group 3-18
show lldp command 6-13
show logging console command 7-17
show logging info command 7-18
show logging last command 7-20
show logging level command 7-21

Send feedback to nexus4K-docfeedback@cisco.com

show logging logfile command 7-22
show logging module command 7-24
show logging monitor command 7-25
show logging nvram command 7-26
show logging onboard command 7-27
show logging server command 7-31
show logging timestamp command 7-32
show mac access-lists command 5-88
show mac-address-table aging-time command 3-20
show mac-address-table command 3-23
show mac-address-table count command 3-21
show mac-address-table notification command 3-22
show module command 1-107
show monitor session command 3-25
show ntp peers command 7-33
show ntp statistics command 7-34
show policy-map command 4-39
show policy-map interface brief command 4-43
show policy-map interface command 4-41
show policy-map type network-qos command 6-15
show policy-map type queuing command 6-17
show port-channel load-balance command 3-26
show port-channel summary command 3-27
show processes command 1-108
show processes cpu command 1-109
show processes log command 1-110
show processes memory command 1-111
show queuing interface command 4-45
show radius-server command 5-89
show role command 5-92
show role feature command 5-94
show role feature-group command 5-97
show running-config aaa command 5-98
show running-config command 1-112, 3-28
show running-config diff command 1-113
show running-config ipqos command 4-47
show running-config radius command 5-100
show running-config security command 5-102
show running-config spanning-tree command 3-29
show running-config tacacs+ command 5-104
show running-config vlan command 3-30
show solm cin command 3-31
show solm counters command 3-32
show spanning-tree active command 3-37
show spanning-tree bridge command 3-38
show spanning-tree brief command 3-40
show spanning-tree command 3-34
show spanning-tree detail command 3-41
show spanning-tree interface command 3-42
show spanning-tree mst command 3-44
show spanning-tree mst configuration command 3-46
show spanning-tree mst detail command 3-47
show spanning-tree mst interface command 3-48
show spanning-tree root command 3-49
show spanning-tree summary command 3-50
show spanning-tree vlan active command 3-52
show spanning-tree vlan bridge command 3-53
show spanning-tree vlan brief command 3-55
show spanning-tree vlan command 3-51
show spanning-tree vlan detail command 3-57
show spanning-tree vlan interface command 3-58
show spanning-tree vlan root command 3-60
show spanning-tree vlan summary command 3-62
show sprom command 1-115
show ssh key command 5-106
show ssh server command 5-108
show startup-config aaa command 5-109
show startup-config command 1-118
show startup-config radius command 5-110
show startup-config security command 5-111
show startup-config tacacs+ command 5-112
show switchname command 1-120
show system cores command 1-121
show system internal sysmgr startup-config locks command 1-122
show system reset-reason command 1-123
show system uptime command 1-124
show tacacs+ command 1-125

Send feedback to nexus4K-docfeedback@cisco.com

show tacacs-server command 5-113
show tech-support command 1-126
show telnet server command 5-116
show terminal command 1-128
show udld command 3-63
show user-account command 5-117
show users command 5-119
show version command 1-129
show vlan access-list command 5-120
show vlan access-map command 5-121
show vlan command 3-64
show vlan filter command 5-122
show vlan id command 3-66
show vlan private-vlan command 3-67
show vrf command 7-36
shutdown (VLAN configuration) command 2-51
sleep command 1-131
spanning-tree bpdufilter command 2-53
spanning-tree bpduguard command 2-54
spanning-tree cost command 2-56
spanning-tree guard command 2-58
spanning-tree link-type command 2-59
spanning-tree loopguard default command 2-60
spanning-tree mode command 2-61
spanning-tree mst configuration command 2-62
spanning-tree mst cost command 2-64
spanning-tree mst forward-time command 2-66
spanning-tree mst hello-time command 2-67
spanning-tree mst max-age command 2-68
spanning-tree mst max-hops command 2-69
spanning-tree mst port-priority command 2-70
spanning-tree mst priority command 2-71
spanning-tree mst root command 2-72
spanning-tree mst simulate pvst command 2-74
spanning-tree mst simulate pvst global command 2-76
spanning-tree pathcost method command 2-78
spanning-tree port-priority command 2-91
spanning-tree port type edge bpdufilter default command 2-81
spanning-tree port type edge bpduguard default command 2-83
spanning-tree port type edge command 2-79
spanning-tree port type edge default command 2-85
spanning-tree port type network command 2-87
spanning-tree port type network default command 2-89
spanning-tree vlan command 2-92
speed (Ethernet) command 2-94
speed command 1-132
ssh command 5-123
ssh key command 5-124
ssh server enable command 5-126
state command 2-95
statistics per-entry command 5-127
stopbits command 1-133
storm-control command 5-128
switchname command 1-134
switchport access vlan command 2-96
switchport block command 2-97
switchport mode private-vlan host command 2-98
switchport mode private-vlan promiscuous command 2-99
switchport mode trunk command 6-18
switchport private-vlan host-association command 2-100
switchport private-vlan mapping command 2-102
switchport trunk allowed vlan command 6-19
system cores command 1-135
system jumbomtu command 4-49
system message logging facilities 7-37
system message severity levels 7-5
system qos command 4-50
system startup-config unlock command 1-136

T

tacacs-server deadtime command 5-130
tacacs-server directed-request command 5-131
tacacs-server host command 5-132
tacacs-server key command 5-134

Send feedback to nexus4K-docfeedback@cisco.com

tacacs-server timeout command 5-135
tail command 1-137
TCP ports 5-23
telnet command 5-136
telnet server enable command 5-137
terminal length command 1-138
terminal session-timeout command 1-139
terminal terminal-type command 1-140
terminal width command 1-141
traceroute command 1-142

U

udld (configuration mode) command 2-104
udld (Ethernet) command 2-106
UDP ports 5-24
update license command 1-143
username command 5-140
use-vrf command 5-138

V

vlan (EXEC mode) command 2-108
vlan access-map command 5-142
vlan filter command 5-143
vlan policy deny command 5-145
vrf context command 7-39
vrf policy deny command 5-146

W

write erase command 1-144

Send feedback to nexus4K-docfeedback@cisco.com