

Network OS

Command Reference

Supporting Network OS v2.0

BROCADE

Copyright © 2010 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, TurboIron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, and VCS are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters Brocade Communications Systems, Inc.

San Jose, CA 95134 Tel: 1-408-333-8000 Fax: 1-408-333-8101 E-mail: info@brocade.com

130 Holger Way

European Headquarters Brocade Communications Switzerland Sàrl Centre Swissair Tour B - 4ème étage 29, Route de l'Aéroport

Case Postale 105
CH-1215 Genève 15
Switzerland

Tel: +41 22 799 5640 Fax: +41 22 799 5641

E-mail: emea-info@brocade.com

Asia-Pacific Headquarters

Brocade Communications Systems China HK, Ltd.

No. 1 Guanghua Road Chao Yang District Units 2718 and 2818 Beijing 100020, China Tel: +8610 6588 8888 Fax: +8610 6588 9999 E-mail: china-info@brocade.com

Asia-Pacific Headquarters

Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)

Citic Plaza

No. 233 Tian He Road North Unit 1308 – 13th Floor Guangzhou, China Tel: +8620 3891 2000 Fax: +8620 3891 2111

E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Network OS Command Reference	53-1002081-01	New document	December 2010

Contents

About This Document In this chapter xv How this document is organized xv Supported hardware and software xv What's new in this document.....xvi Document conventions.....xvi Command syntax conventions xvi Notes, cautions, and warnings xvii Key terms xvii Notice to the readerxvii Additional information. xviii Brocade resources.....xviii Other industry resources xviii Getting technical help.....xviii Document feedback xix Chapter 1 Using the Network OS CLI Network OS CLI keyboard shortcuts......5 Displaying Network OS CLI commands and command syntax . . 5 Network OS CLI command completion......7 Chapter 2 Network OS Commands aaa authentication......9 advertise dcbx-fcoe-logical-link-tlv11 advertise dcbx-isci-app-tlv......12

advertise dcbx-tlv......13

advertise dot1-tlv14
advertise dot3-tlv15
advertise optional-tlv
advertisement interval (fabric-map)17
arp-ageing-timeout18
associate19
banner login
bridge-priority
cee22
cee-map (Configuration)
cee-map (FCoE)
channel-group25
chassis disable26
chassis enable
cisco-interoperability
clear arp-cache29
clear counters30
clear counters access-list mac
clear dot1x statistics
clear dot1x statistics interface
clear fcoe login34
clear ip fib35
clear ip igmp groups36
clear ip traffic37
clear lacp38
clear lacp counters39
clear lldp neighbors
clear IIdp statistics41
clear logging raslog42
clear spanning-tree counter
clear support44
clock set45
clock timezone
copy47
copy (AMPP)
copy default-config startup-config
copy running-config startup-config

copy support	.52
debug arp	.53
debug ip	.54
debug ip igmp	.55
debug lacp	.56
debug Ildp packet	.58
debug spanning-tree	.59
delete	.60
deny (extended ACLs)	. 61
deny (standard ACLs)	.63
description (interfaces)	.64
description (LLDP)	.65
description (Port Mirroring)	.66
diag burninerrclear	.67
diag clearerror	.68
diag portledtest	.69
diag portloopbacktest	.70
diag post	. 71
diag setcycle	.72
diag systemverification	.73
diag turboramtest	. 74
dir	.75
dot1x authentication	. 76
dot1x enable	.77
dot1x port-control	.78
dot1x quiet-period	.79
dot1x reauthenticate interface	.80
dot1x reauthentication	. 81
dot1x reauthMax	.82
dot1x timeout re-authperiod	.83
dot1x timeout server-timeout	.84
dot1x timeout supp-timeout	.85
dot1x timeout tx-period	.86
dpod	. 87
end	.88
error-disable-timeout enable	.89
error-disable-timeout interval	90

exit91
fabric isl enable92
fabric route multicast
fabric trunk enable94
fabric-map95
fastboot96
fcmap97
fcoe98
fcoeport map99
fcoe-profile (AMPP)100
firmware commit101
firmware download102
firmware restore104
forward-delay105
hello106
hello-time
instance
interface
interface fcoe
interface management111
interface vlan
ip address114
ip igmp last-member-query-interval
ip igmp query-interval116
ip igmp query-max-response-time117
ip igmp snooping enable (global version)118
ip igmp snooping enable (VLAN version)
ip igmp snooping fast-leave120
ip igmp snooping mrouter
ip igmp snooping mrouter-timeout
ip igmp snooping querier enable123
ip igmp static-group
keep-alive timeout (fabric-map)
12traceroute
lacp system-priority129
lacp timeout
license add

license remove	132
line vty exec-timeout	
Ildp dcbx-version	
Ildp disable	
Ildp iscsi-priority	136
Ildp profile	
logging switchid raslog console	
logging syslog-server	
mac access-group	140
mac access-list extended	141
mac access-list standard	142
mac-address-reduction	143
mac-address-table	144
map	145
max-age	146
max-hops	147
minimum-links	148
mode	149
monitor session	150
mtu	151
multiplier	152
ntp server	153
password-attributes	154
permit (extended ACLs)	156
permit (standard ACLs)	158
port-channel path-cost	159
port-profile	160
port-profile-port	161
precedence	162
priority	163
priority-group-table	164
priority-table	165
profile	167
protect-mode enable	168
protocol Ildp	169
protocol spanning-tree	170
bwd	171

qos cos
qos cos-mutation
qos cos-traffic-class
qos flowcontrol
qos flowcontrol pfc cos
qos map cos-mutation
qos map cos-traffic-class
qos-profile (AMPP)
qos queue multicast scheduler180
qos queue scheduler
qos rcv-queue multicast rate-limit
qos rcv-queue multicast threshold
qos trust cos
radius-server188
region
reload
remap fabric-priority192
remap lossless-priority193
rename
resequence access-list mac
revision
rmon alarm197
rmon collection history198
rmon collection stats
rmon event
role name
rule
run-script
security-profile (AMPP)204
seq (extended MAC ACLs)
seq (standard MAC ACLs)207
service password-encryption208
sflow collector
sflow enable (global version)
sflow enable (interface version)
sflow polling-interval (global version)
sflow polling-interval (interface version)213

sflow	sample-rate (global version)	214
sflow	sample-rate (interface version)	215
show	accounting logs2	216
show	arp2	217
show	calendar2	218
show	cee maps2	219
show	chassis2	20
show	clock2	22
show	debug ip igmp2	23
show	debug lacp	224
show	debug lldp2	25
show	debug spanning-tree	26
show	diag burninerrshow2	227
show	diag burninstatus2	28
show	diag post results2	29
show	diag setcycle	30
show	diag status2	231
show	dot1x2	32
show	dot1x all2	33
show	dot1x diagnostics interface	34
show	dot1x interface	35
show	dot1x session-info interface	36
show	dot1x statistics interface	237
show	dpod	38
show	environment	39
show	environment fan	240
show	environment history	241
show	environment power	43
show	environment sensor	244
show	environment temp	245
show	fabric all2	246
show	fabric isl2	247
show	fabric islports	248
show	fabric route multicast	50
show	fabric route topology2	52
show	fabric trunk	54
show	fcoe fabric-map	55

show fcoe interface	256
show fcoe login	257
show fcoe map	258
show file	259
show firmwaredownloadstatus	260
show interface	261
show interface management	263
show ip fib	264
show ip forwarding	265
show ip igmp groups	266
show ip igmp snooping	267
show ip interface	268
show lacp counter	270
show lacp-sys-id	271
show license	272
show license id	274
show IIdp interface	275
show lldp neighbors	276
show IIdp statistics	278
show logging	279
show logging raslog	280
show mac access-group	281
show mac-address-table	282
show media	284
show media interface	285
show media linecard	286
show monitor	287
show name-server	288
show ntp status	289
show port-channel	290
show port-profile	291
show port-profile interface	292
show port-profile status	293
show process	294
show processes cpu	296
show processes memory	297
show protect-mode status	298

show	qos flowcontrol interface	299
show	qos interface.	300
show	qos maps	302
show	qos queue interface	303
show	qos rcv-queue interface	304
show	qos rcv-queue multicast	305
show	rmon	306
show	rmon history	308
show	running-config.	309
show	running-config aaa	310
show	running-config banner	311
show	running-config dpod	312
show	running-config fabric route mcast	313
show	running-config fcoe	314
show	running-config igmp	315
show	running-config interface management	316
show	running-config logging	317
show	running-config logging syslog-server	318
show	running-config password-attributes	319
show	running-config radius-server	320
show	running-config role	321
show	running-config rule	322
show	running-config snmp-server	323
show	running-config tacacs-server	324
show	running-config username	325
show	running-config switch-attributes	326
show	running-configuration diag post	327
show	sflow	328
show	spanning-tree	329
show	spanning-tree brief	331
show	spanning-tree interface	332
show	spanning-tree mst brief	333
show	spanning-tree mst detail	334
show	spanning-tree mst instance	337
show	spanning-tree mst interface	338
show	startup-config	339
show	startup-config fcoe	340

show statistics access-list mac341
show support
show system344
show tech-support
show users
show vcs
show version
show vlan349
show vlan classifier350
shutdown351
shutdown (STP)352
snmp-server community353
snmp-server contact354
snmp-server host
snmp-server location
spanning-tree autoedge357
spanning-tree bpdu-mac
spanning-tree cost
spanning-tree edgeport360
spanning-tree guard root361
spanning-tree hello-time
spanning-tree instance
spanning-tree link-type
spanning-tree portfast365
spanning-tree priority366
spanning-tree restricted-role
spanning-tree restricted-tcn
spanning-tree shutdown
spanning-tree tc-flush-standard370
speed371
support372
switch-attributes373
switchport374
switchport access
switchport mode converged376
switchport mode377
switchport trunk378

system-description379
system-name
tacacs-server
terminal length383
terminal monitor
transmit-holdcount
unlock username
usb dir
usb off
usb on
usb remove
username
vcs
vepa enable
virtual-fabric
vlan classifier activate group
vlan classifier group
vlan classifier rule
vlan-profile (AMPP)

About This Document

In this chapter

• How this document is organized	ΧV
Supported hardware and softwarex	ΚV
• What's new in this document	vi
Document conventions	vi
Notice to the reader	۷ij
• Additional information	iii
• Getting technical help	iii
Document feedback	ίx

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, "Using the Network OS CLI," explains how to use the command line interface.
- Chapter 2, "Network OS Commands," provides command information.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS 2.0.0, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Network OS:

- Brocade VDX 6720
 - Brocade VDX 6720-24
 - Brocade VDX 6720-60

What's new in this document

This is a new document.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text Identifies command names

Identifies the names of user-manipulated GUI elements

Identifies keywords and operands
Identifies text to enter at the GUI or CLI

italic text Provides emphasis

Identifies variables

Identifies paths and Internet addresses

Identifies document titles

Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is all lowercase.

Command syntax conventions

Command syntax in this manual follows these conventions:

Convention	vention Description	
[]	Keywords or arguments that appear within square brackets are optional.	
{x y z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.	
screen font	Examples of information displayed on the screen.	
<>	Nonprinting characters, for example, passwords, apear in angle brackets.	
[]	Default responses to system prompts appear in square brackets.	
italic text	Identifies variables.	
bold text	Identifies literal command options.	

NOTE

In standalone mode, interfaces are identified using slot/port notation. In VCS mode, interfaces are identified using switch/slot/port notation.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE

A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates potential damage to hardware or data.



CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on MyBrocade. See "Brocade resources" on page xviii for instructions on accessing MyBrocade.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

TABLE 1

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Oracle Corporation	Oracle, Java
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to http://my.brocade.com to register at no cost for a user ID and password.

White papers, online demonstrations, and data sheets are available through the Brocade website at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Release notes are available on the MyBrocade website.

Other industry resources

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

- 1. General Information
 - Switch model
 - Switch operating system version
 - Software name and software version, if applicable
 - Error numbers and messages received
 - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
 - Description of any troubleshooting steps already performed and the results
 - Serial console and Telnet session logs
 - syslog message logs

2. Switch Serial Number

The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below:



The serial number label is located as follows:

 Brocade VDX 6720—On the switch ID pull-out tab located on the bottom of the port side of the switch

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Using the Network OS CLI

1

In this chapter

 DCB command line interface		
---	--	--

DCB command line interface

The Brocade Data Center Bridging (DCB) CLI is designed to support the management of DCB and Layer 2 Ethernet switching functionality. The Network OS CLI uses an industry-standard hierarchical shell familiar to Ethernet/IP networking administrators.

The system starts up with the default Network OS configuration and the DCB startup configuration. After logging in, you are in the Network OS shell. For information on accessing the DCB commands from the Network OS shell, see "Network OS CLI command modes" on page 2.

Saving your configuration changes

Any configuration changes made to the switch are written into the running-config file. This is a dynamic file that is lost when the switch reboots. During the boot sequence, the switch resets all configuration settings to the values in the startup-config file.

To make your changes permanent, use the **copy** command to commit the running-config file to the startup-config file, as shown below.

Example of committing the running-config in privileged EXEC mode.

switch#copy running-config startup-config

Network OS CLI RBAC permissions

Role-Based Action Control (RBAC) defines the capabilities that a user account has based on the role the account has been assigned.

A role is an entity that defines the access privileges of the user accounts on the switch. A user is associated with one role. Refer to the *Network OS Administrator's Guide* for information about RBAC.

Default roles

Attributes of default roles cannot be modified; however, the default roles can be assigned to non-default user accounts. The following roles are default roles:

 The admin role has the highest privileges. All CLIs are accessible to the user associated with the admin role. By default, the admin role has read and write access. The user role has limited privileges that are mostly restricted to show commands in the Privileged EXEC mode. User accounts associated with the user role cannot access configuration CLIs that are in the global configuration mode. By default, the user role has read-only access.

Accessing the Network OS CLI through Telnet

NOTE

While this example uses the admin role to log in to the switch, both roles can be used.

The procedure to access the Network OS CLI is the same through either the console interface or through a Telnet session; both access methods bring you to the login prompt.

```
switch login: admin
Password:*******
switch#
```

NOTE

Multiple users can Telnet sessions and issue commands using the privileged EXEC mode. Network OS v2.0.0 supports up to 32 Telnet sessions with the admin login.

Network OS CLI command modes

Figure 1 displays the Network OS CLI command mode hierarchy.

FIGURE 1 Network OS CLI command mode hierarchy

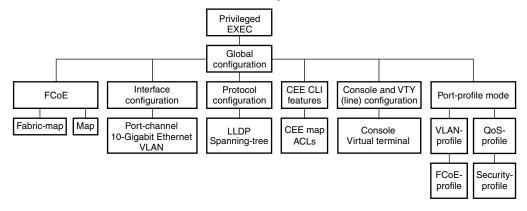


Table 2 lists the Network OS CLI command modes and describes how to access them.

NOTE

Use the **pwd** command to view the mode of the current working directory. This command functions in global configuration mode and the modes accessed from global configuration mode.

TABLE 2 Network OS CLI command modes

Command mode	Prompt	How to access the command mode	Description
Privileged EXEC	switch#	This is the default mode for the switch.	Display and change system parameters. Note that this is the administrative mode and includes the basic configuration commands.
Global configuration	switch(config)#	From the privileged EXEC mode, enter the configure terminal command.	Configure features that affect the entire switch.
Interface configuration	Port-channel: switch(config-Port-channel-63)# 10-Gigabit Ethernet (DCB port): switch(conf-if-te-0/1)#	From the global configuration mode, specify an interface by entering one of the following commands: interface port-channel interface tengigabitethernet interface vlan	Access and configure individual interfaces.
	VLAN: switch(conf-Vlan-1)#		
Protocol configuration	LLDP: switch(conf-lldp)#	From the global configuration mode, specify a protocol by entering one of the following commands:	Access and configure protocols.
	<pre>Spanning-tree: switch(conf-mstp)# switch(conf-rstp)# switch(conf-stp)# switch(conf-pvst)# switch(conf-rpvst)#</pre>	 protocol IIdp protocol spanning-tree mstp protocol spanning-tree rstp protocol spanning-tree stp protocol spanning-tree pvst protocol spanning-tree rapid-pvst 	
FCoE configuration	FCoE: switch(config-fcoe)#	From the global configuration mode, use the fcoe command to enter FCoE configuration mode.	Access and configure FCoE features.
	<pre>FCoE fabric-map sub-mode: switch(config-fcoe-fabric-map)#</pre>	From the FCoE configuration mode, specify an FCoE sub-mode by	
	<pre>FCoE map sub-mode: switch(config-fcoe-map)#</pre>	entering one of the following commands: fabric-map default map default	

TABLE 2 Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description
AMPP	AMPP port-profile:	From the global configuration mode,	Access and configure AMPP
port-profile mode	<pre>switch(conf-port-profile-name)#</pre>	enter the port-profile command to enter port-profile configuration	features.
	VLAN-profile sub-mode:	mode.	
	switch(conf-vlan-profile)#		
	<pre>QoS-profile sub-mode: switch(conf-qos-profile)#</pre>	From the port-profile configuration mode, specify an AMPP sub-mode by entering one of the following	
	FCoE-profile sub-mode: switch(conf-fcoe-profile)#	commands: vlan-profile qos-profile fcoe-profile	
	Security-profile sub-mode: switch(conf-security-profile)#	security-profile	
Feature configuration	CEE map:	From the global configuration mode,	Access and configure CEE map
	switch(config-cee-map-default)#	specify a DCB feature by entering one of the following commands:	features.
	Standard ACL:	cee-map default	
	switch(conf-macl-std)#	mac access-list standardmac access-list extended	
	Extended ACL:		
	switch(conf-macl-ext)#		

NOTE

Pressing **Ctrl+Z** or entering the **end** command in any mode returns you to privileged EXEC mode. Entering **exit** in any mode returns you to the previous mode.

Network OS CLI keyboard shortcuts

Table 3 lists Network OS CLI keyboard shortcuts.

TABLE 3 Network OS CLI keyboard shortcuts

Keystroke	Description
Ctrl+B or the left arrow key	Moves the cursor back one character.
Ctrl+F or the right arrow key	Moves the cursor forward one character.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl+Z	Returns to privileged EXEC mode.
Ctrl+P or the up arrow key	Displays commands in the history buffer with the most recent command displayed first.
Ctrl+N or the down arrow key	Displays commands in the history buffer with the most recent command displayed last.

NOTE

In privileged EXEC mode, use the **show history** command to list the commands most recently entered. The switch retains the history of the last 1000 commands entered from all terminals.

Using the do command as a shortcut

You can use the **do** command to save time when you are working in any configuration mode and you want to run a command in privileged EXEC mode.

For example, if you are configuring LLDP and you want to execute a privileged EXEC mode command, such as the **dir** command, you would first have to exit the LLDP configuration mode. By using the **do** command with the **dir** command, you can ignore the need to change configuration modes, as shown in the following example.

Displaying Network OS CLI commands and command syntax

Enter a question mark (?) in any command mode to display the list of commands available in that mode.

```
do
                  Run an operational-mode command
exit
                  Exit from current mode
hello
                   The Hello Transmit interval.
help
                  Provide help information
iscsi-priority Configure the Ethernet priority to advertise for iSCSI
                   The LLDP mode.
multiplier
                  The Timeout Multiplier
                  Negate a command or set its defaults
no
profile
                   The LLDP Profile table.
                   Display current mode path
pwd
system-description The System Description.
system-name
                   The System Name
top
                   Exit to top level and optionally run command
```

To display a list of commands that start with the same characters, type the characters followed by the question mark (?).

```
switch#e?
Possible completions:
   exit    Exit the management session
```

To display the keywords and arguments associated with a command, enter the keyword followed by the question mark (?).

If the question mark (?) is typed within an incomplete keyword, and the keyword is the only keyword starting with those characters, the CLI displays help for that keyword only.

```
switch#show d?
Possible completions:
  debug    Debug
  diag    Show diag related information
  dot1x    Show dot1x
  dpod    Provides License Information on Pod in fabric
```

If the question mark (?) is typed within an incomplete keyword but the keyword matches several keywords, the CLI displays help for all the matching keywords.

The Network OS CLI accepts abbreviations for commands. This example is the abbreviation for the **show qos interface all** command.

```
switch#sh q i a
```

If the switch does not recognize a command after **Enter** is pressed, an error message displays.

If an incomplete command is entered, an error message displays.

Network OS CLI command completion

To automatically complete the spelling of commands or keywords, begin typing the command or keyword and then press **Tab**. For example, at the CLI command prompt, type **te** and press **Tab**:

```
switch#te
```

The CLI displays the following command.

```
switch#terminal
```

If there is more than one command or keyword associated with the characters typed, the Network OS CLI displays all choices. For example, at the CLI command prompt, type **show I** and press **Tab**:

```
switch#show 1
```

The CLI displays the following command.

Network OS CLI command output modifiers

You can filter the output of the Network OS CLI **show** commands using the output modifiers described in Table 4. Use the pipe character (|) to add these modifiers.

TABLE 4 Network OS CLI command output modifiers

Output modifier	Description	
redirect	Redirects the command output to the specified file.	
include	Displays the command output that includes the specified expression.	
exclude	Displays the command output that excludes the specified expression.	
append	Appends the command output to the specified file.	
begin	Displays the command output that begins with the specified expression.	
last	Displays only the last few lines of the command output.	
tee	Redirects the command output to the specified file. Note that this modifier also displays the command output.	

1 DCB command line interface

Chapter

2

Network OS Commands

aaa authentication

Specifies the server that is used for authentication, authorization, and accounting (AAA) on the

switch.

Synopsis aaa authentication login {default | radius | tacacs+ | local }

no aaa authentication login

Operands login

default | radius | tacacs+ | local

Specifies the type of server that will be used for authentication,

authorization, and accounting on the switch. The local server is the default.

Description Use this command to select the type of server that will be used for AAA on a selected switch.

Default The default source is local.

Command Modes Global configuration mode

Usage Guidelines There are no usage guidelines for this command.

Examples switch(config)# aaa authentication login ?

Possible completions:

default local radius tacacs+

switch(config)# aaa authentication login tacacs+ ?

Possible completions:

radius local

See Also show running-config aaa

advertise dcbx-fcoe-app-tlv

Advertises application Type, Length, Values (TLVs) to ensure interoperability of traffic over the Data Center Bridging eXchange protocol (DCBX), which runs over LLDP to negotiate an FCoE application

TLV.

Synopsis advertise dcbx-fcoe-app-tlv

no advertise dcbx-fcoe-app-tlv

Operands None

Defaults Advertise is disabled.

Command Modes Protocol LLDP configuration mode

Description Use this command to advertise application TLVs to ensure interoperability of traffic over DCBX

packets. Converged Enhanced Ethernet (CEE) parameters related to FCoE must be negotiated before FCoE traffic can begin on a CEE link. An FCoE application TLV is exchanged over LLDP, which negotiates information such as FCoE priority, and Priority Flow Control (PFC) pause. Use the

no advertise dcbx-fcoe-app-tlv command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also advertise dot1-tlv, advertise dot3-tlv, advertise optional-tlv

advertise dcbx-fcoe-logical-link-tlv

Advertises to any attached device the FCoE status of the logical link.

Synopsis advertise dcbx-fcoe-logical-link-tlv

no advertise dcbx-fcoe-logical-link-tlv

Operands None

Defaults Advertise is disabled.

Command Modes Protocol LLDP configuration mode

Description Use this command to advertise to any attached device the FCoE status of the logical link.

Use the no advertise dcbx-fcoe-logical-link-tlv command to return to the default setting.

Examples None

See Also advertise dcbx-fcoe-app-tlv

2

advertise dcbx-isci-app-tlv

Advertises the iSCSI traffic configuration parameters for TLV.

Synopsis advertise dcbx-isci-app-tlv

no advertise dcbx-isci-app-tlv

Operands None

Defaults Advertise is enabled.

Command Modes Protocol LLDP configuration mode

Description Advertises the iSCSI traffic configuration parameters to the attached CEE-enabled servers and

targets. No verification or enforcement of the usage of the advertised parameters by the iSCSI

server or target is done by the switch.

Use the no advertise dcbx-isci-app-tlv command to return to the default setting.

Examples None

See Also advertise dcbx-fcoe-app-tlv

advertise dcbx-tlv

Advertises to any attached device mandatory Data Center Bridging eXchange protocol (DCBX)

Type, Length, Values (TLVs).

Synopsis advertise dcbx-tlv

no advertise dcbx-tlv

Operands None

Defaults Advertise is enabled.

Command Modes Protocol LLDP configuration mode

Description Advertises to any attached device mandatory Data Center Bridging eXchange protocol (DCBX)

Type, Length, Values (TLVs). Use the **no advertise dcbx-tlv** command to return to the default

setting.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also advertise dot1-tlv, advertise dot3-tlv, advertise optional-tlv

2

advertise dot1-tlv

Advertises to any attached device IEEE 802.1 organizationally specific Type, Length, Value (TLV).

Synopsis advertise dot1-tlv

no advertise dot1-tlv

Operands None

Defaults Advertise is disabled.

Command Modes Protocol LLDP configuration mode

Description Use this command to advertise to any attached device IEEE 802.1 organizationally specific Type,

Length, Value (TLV). Use the no advertise dot1-tlv command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also advertise dcbx-tlv, advertise dot3-tlv, advertise optional-tlv

advertise dot3-tlv

Advertises to any attached device IEEE 802.3 organizationally specific Type, Length, Value (TLV).

Synopsis advertise dot3-tlv

no advertise dot3-tlv

Operands None

Defaults Advertise is disabled.

Command Modes Protocol LLDP configuration mode

Description Use this command to advertise to any attached device IEEE 802.3 organizationally specific Type,

Length, Value (TLV). Use the no advertise dot3-tlv command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also advertise dcbx-tlv, advertise dot1-tlv, advertise optional-tlv

advertise optional-tlv

Advertises the optional Type, Length, and Value (TLV)s.

Synopsis advertise optional-tlv [management-address | port-description | system-capabilities |

system-description | system-name]

no advertise optional-tlv

Operands management-address

Advertises the management address of the system.

port-description Advertises the user-configured port.

system-capabilities Advertises the capabilities of the system.

system-description Advertises the system firmware version and the current image running on

the system.

system-name Advertises the name of the system.

Defaults Advertise is disabled.

Command Modes Protocol LLDP configuration mode

Description Use this command to display the following optional TLVs.

Examples None

See Also advertise dcbx-tlv, advertise dot1-tlv, advertise dot3-tlv

advertisement interval (fabric-map)

Configures the advertisement interval.

Synopsis advertisement interval milliseconds

no advertisement interval

Operands milliseconds The interval value in milliseconds. The range of valid values is from 250

through 9000 milliseconds.

Defaults The default value is 8000 milliseconds.

Command Modes FCoE fabric-map configuration mode

Description Use this command to configure the advertisement interval for the FCoE fabric-map mode.

Use no advertisement interval to reset the value to 8000 milliseconds.

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Examples switch(config)#fcoe

switch(config-fcoe)#fabric-map default

switch(config-fcoe-fabric-map)#advertisement interval 8000

See Also fcoe

2

arp-ageing-timeout

Defines the ARP ageing timeout value in seconds.

Synopsis arp-ageing-timeout minutes

no arp-ageing-timeout

Operands *minutes* Number of minutes until the timeout occurs.

Defaults Default value is 240 minutes (four hours).

Command Modes Global configuration mode

Description Use this command to configure the ARP timeout.

Usage Guidelines Use **no arp-ageing-timeout** to disable this function.

Examples None

associate

Associates a MAC address to the port-profile.

Synopsis associate addr mac_addr vlan vlan_id pp profile-name

Operands addr mac_addr Specifies the server MAC address.

vian *vlan_id* Specifies the VLAN number. The range of valid values is from 1 through

4094.

pp profile-name Specificies the port-profile to associate.

Defaults There are no defaults for this command.

Command Modes Port-profile mode

Description You can associate the MAC with an active port-profile. When the associated MAC appears on

aprofiled-port then the corresponding configuration from the associated port-profile is applied onthat profiled-port, assuming there are no-conflicts with an already existing port-profile

A MAC can be associated to only one port-profile.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

banner login

Sets the login banner.

Synopsis banner login message

no banner login message

Operands message Specifies a text string to be displayed upon login. The string must be

enclosed in double quotation marks. The maximum length is 1022

characters.

Defaults None

Command Modes Global configuration mode

Description Use this command to set the banner on the local switch.

The banner is a string of alphanumeric characters. It is displayed whenever you log in to a switch.

Use the **no banner login** command to remove the banner.

Usage Guidelines This command is supported only on the local switch.

Examples To set a new banner for a switch:

switch(config)#banner login "Please don't disturb the setup on this switch."

switch(config)#exit

Login as: admin
Password: *****

Please don't disturb the setup on this switch.

Welcome to the Brocade Network Operating System Software

adminconnected from 10.120.34.144 using ssh on sw0

See Also clear support, show support, vcs, firmware download, firmware restore, interface management

bridge-priority

Specifies the priority of the bridge.

Synopsis bridge-priority priority vlan_id

no bridge-priority

Operands priority Specifies the bridge priority. The range of valid values is from 0 through

61440.

vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults The default priority is 32678.

Command Modes Protocol Spanning Tree mode

Description Use this command to set the bridge priority for the common instance. Using a lower priority value

indicates that the bridge might become root. Use the no bridge-priority command to return to the

default settings.

Usage Guidelines This command must be used to specify the priority of the bridge. The priority values can be set only

in increments of 4096.

Examples To specify the bridge priority:

 $\verb|switch| \# \textbf{configure terminal}| \\$

switch(config)#protocol spanning-tree stp
switch(conf-stp)#bridge-priority 8192

switch#configure terminal

switch(config)#protocol spanning-tree rstp
switch(conf-rstp)#bridge-priority 8192

switch#configure terminal

switch(config)#protocol spanning-tree mstp
switch(conf-mstp)#bridge-priority 8192

See Also protocol spanning-tree

2 cee

cee

Applies a CEE provisioning map on an interface.

Synopsis cee default

no cee

Operands None

Defaults There is no CEE Provisioning applied on an interface. The only map name allowed is "default."

Command Modes Interface configuration mode

Description Use this command to apply the CEE map on an interface. Use the **no cee** command to remove the

CEE Provisioning map.

Usage Guidelines The CEE map applied on an interface should already exist on the switch.

Examples To apply a the CEE map to an interface:

switch(conf-if-te-0/1)#cee default

See Also cee-map (Configuration)

cee-map (Configuration)

Enters the CEE map configuration mode.

Synopsis cee-map default

Operands None

Defaults The only map name allowed is "default."

Command Modes Global configuration mode

Description Only a single CEE map is allowed, named "default." It is created when system starts up. The initial

configuration of the default CEE map is:

```
Precedence 1
  Priority Group Table
    1: Weight 40, PFC Enabled, TrafficClass 3, BW% 40
    2: Weight 60, PFC Disabled, TrafficClass 6, BW% 60
    15.0: PFC Disabled
    15.1: PFC Disabled
    15.2: PFC Disabled
    15.3: PFC Disabled
    15.4: PFC Disabled
    15.5: PFC Disabled
    15.6: PFC Disabled
    15.7: PFC Disabled
  Priority Table
     CoS: 0
                1 2 3 4
                                   5
                                            7
    PGID:
            2
                 2 2 1 2 2 2
  FCoE CoS: None
  Enabled on the following interfaces
```

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also cee, fcoeport map, priority-group-table, priority-table

2

cee-map (FCoE)

Assigns a cee-map to the FCoE Fabric-Map.

Synopsis cee-map default

Operands None

Defaults The only map name allowed is "default."

Command Modes FCoE map configuration mode

Description This command assigns a cee-map to the FCoE fabric-map.

Usage Guidelines Use **no cee-map** to revert to the default values for the map.

You must be in the feature configuration mode for FCoE map for this command to function.

Examples switch(config)#fcoe

switch(config-fcoe)#map default

switch(config-fcoe-map)#cee-map default

See Also fabric-map, fcoe

channel-group

Enables Link Aggregation on an interface.

Synopsis channel-group number mode [active | passive | on] [type standard | brocade]

no channel-group

Operands number Specifies a Link Aggregation Group (LAG) port channel-group number to

which this link should administratively belong to. The range of valid values is

from 1 through 63.

mode Specifies the mode of Link Aggregation.

active Enables the initiation of LACP negotiation on an interface.

passive Disables LACP on an interface.

on Enables static link aggregation on an interface.

type Specifies the type of LAG.

standard Specifies the 802.3ad standard-based LAG.

brocade Specifies the Brocade proprietary hardware-based trunking.

Defaults By default, the type is set to standard.

Command Modes Interface configuration mode

Description

Use this command to add an interface to a port-channel specified by the channel-group number. This command enables link aggregation on an interface, so that it may be selected for aggregation by the local system. Use the **no channel-group** command to remove the port-channel members.

Usage Guidelines Only a maximum of 24 LAGs can be created. Note the following:

- A maximum of four link aggregation groups can be created per switch when the **type** is set to **brocade**.
- A maximum of four links can become part of a single aggregation group when the **type** is set to **brocade** and they must be on the same port-channel.
- Links 0-7 belong to port-channel 1; links 8-15 belong to port-channel 2, and links 16-23 belong to port-channel 3.
- For the standard type, a maximum of 16 links can be aggregated per aggregation group and they can be members of any port-channel.

Examples To set the channel-group number to 4 and the mode to active:

switch(conf-if)#channel-group 4 mode active

See Also interface

2

chassis disable

Disables all interfaces in the chassis.

Synopsis chassis disable

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to disable all interfaces on the local switch. All interfaces will be taken offline.

Use the chassis disable command before making configuration changes or running offline

diagnostics.

Usage Guidelines This command is supported only on the local switch.

Examples To disable all interfaces on the local switch:

switch# chassis disable

See Also chassis enable

chassis enable

Enables all interfaces in the chassis.

Synopsis chassis enable

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to enable all interfaces on the local switch. All interfaces that passed the

power-on self-test (POST) are enabled. They may come online if connected to a device, or remain offline if disconnected. Use the **chassis enable** command to re-enable the chassis after making

configuration changes or running offline diagnostics.

Usage Guidelines This command is supported only on the local switch.

Examples To enable all interfaces on the local switch:

switch# chassis enable

See Also chassis disable

cisco-interoperability

Configures the switch to interoperate with some legacy Cisco switches.

Synopsis cisco-interoperability [disable | enable]

Operands disable Disables Cisco interoperability for the Multiple Spanning Tree Protocol

(MSTP) switch.

enable Enables Cisco interoperability for the MSTP switch.

Defaults Cisco interoperability is disabled.

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to enable or disable the switch to interoperate with some legacy Cisco

switches. For some switches, the MSTP field Version 3 Length does not adhere to the current

standards.

Usage Guidelines If Cisco interoperability is required on any switch in the network, then all switches in the network

must be compatible, and therefore enabled using this command for interoperability with a Cisco

switch.

Examples To enable Cisco interoperability on a switch:

switch#configure terminal

switch(config)#protocol spanning-tree mstp
switch(conf-mstp)#cisco-interoperability enable

To disable Cisco interoperability on a switch:

 $\verb|switch| \# \textbf{configure terminal}| \\$

switch(config)#protocol spanning-tree mstp

 $\verb|switch(conf-mstp)| \\ \# \textbf{cisco-interoperability disable}|$

clear arp-cache

Clears the ARP statistics cache on the host.

Synopsis clear arp-cache [interface interface-type interface-number [no-refresh]] | [ip ip-address

[no-refresh] | [no-refresh]]

Operands interface Clears the ARP cache for the specified interface only.

interface-type Network interface type (external TenGigabitEthernet interface, null,

port-channel, or VLAN).

interface-number

Layer-2 or layer-3 Interface number.

no-refresh Do not refresh the ARP.

ip Clears the statistics on all interfaces.

ip-address Clear the ARP for this next-hop IP address.

no-refreshno-refreshDo not refresh the ARP.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the ARP statistics cache on the host.

Usage Guidelines There are no usage guidelines for this command.

Examples None

clear counters

Clears statistics on all interfaces on the switch.

Synopsis clear counters [all | access-list mac access_list_name | [interface port-channel number

|tengigabitethernet slot/port | slot-id number] | rmon]

Operands all Specifies to clear statistics on all interfaces.

access_list mac access_list_name

Specifies the name of the MAC access list.

interface Specifies the use of the port-channel, tengigabitethernet, or slot-id keyword.

port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

slot-id *number* Specifies the slot number of the linecard.

rmon Specifies to clear the RMON counters.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear statistics on one or on all interfaces.

Usage Guidelines The clear counters all command does not clear counters for any of the protocol daemon stats like

LLDP, LACP, MSTP, and so on.

For the Brocade 8000 switch, the slot number is always 0 (zero).

Examples To clear the statistics for 10 Gbps Ethernet interface 0/1:

switch#clear counters interface tengigabitethernet 0/1

To clear the statistics for MAC access list named "test":

switch#clear counters access-list mac test

To clear the statistics for all the interfaces on the linecard in slot 0 (zero):

switch#clear counters slot-id 0

See Also show ip fib

clear counters access-list mac

Clears all the Media Access Control (MAC) ACL counters for all interfaces which have ACL applied on them or for a specific interface.

Synopsis clear counters access-list mac name [interface | port-channel number | tengigabitethernet

slot/port | vlan vlan_id]

Operands. name Specifies the name of the MAC ACL.

interface Specifies the use of the port-channel, tengigabitethernet, or vlan keyword.

port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

3583.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear counters for all or for a specific interface for MAC access list counters.

Usage Guidelines If the **interface** keyword is not specified, then ACL counters on all interfaces which have this ACL

applied are cleared. There are 255 ACL counters supported per port group.

Examples To clear counters for the configured MAC access list named test on an interface:

switch#clear counters access-list mac test interface tengiqabitethernet 0/1

To clear counters for the configured MAC access list named test on all interfaces on which this ACL is applied:

switch#clear counters access-list mac test

See Also show mac-address-table, show statistics access-list mac

2

clear dot1x statistics

Clears all dot1x statistics.

Synopsis clear dot1x statistics

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear all accumulated port authentication statistics on all ports.

Usage Guidelines There are no usage guidelines for this command.

Examples To clear dot1x statistics:

switch#clear dot1x statistics

See Also clear dot1x statistics interface

clear dot1x statistics interface

Clears the dot1x statistics for a port

Synopsis clear dot1x statistics interface [tengigabitethernet slot/port]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear all of the dot1x statistics for a specific interface port.

Usage Guidelines There are no usage guidelines for this command.

Examples To clear dot1x statistics on a port:

switch#clear dot1x statistics interface tengigabitethernet 0/16

See Also clear dot1x statistics

clear fcoe login

Clears the FCoE login for a given FCoE interface, vlan, vfid, or device WWN.

Synopsis clear fcoe login [interface fcoe switch/slot/port] | [vlan vlan_id] | [interface tengigabitethernet

switch/slot/port] | [virtual-fabric vfid] | [device device-wwn]

Operands interface fcoe The VN number/VCS node mapped ID/logical port number for the

virtual-fabric.

switch Specifies the switch. This is not valid in standalone mode.

slot Specifies a valid slot number.port Specifies a valid port number.

vlan vlan_id The VLAN ID for the device. The range of valid values is from 1 through 3583.

interface tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

switch Specifies the switch. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

virtual-fabric vfid The virtual fabric ID for the device.device device-wwn The World Wide Name of the device.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description This command clears the FCoE login for a given FCoE interface, vlan, vfid, or device WWN.

Usage Guidelines There are no usage guidelines for this command.

Examples switch#clear fcoe login interface fcoe 1/1/1

switch#clear fcoe login device 10:00:05:1e:8e:be:40
switch#clear fcoe login interface tengigabitethernet 1/0/1

switch#clear fcoe login vlan 1002
switch#clear fcoe login vfid 1

clear ip fib

Clears the FIB and hardware, and then repopulates it.

Synopsis clear ip fib [slot slot-number]

Operands slot slot-number Clears the FIB and hardware for the blade slot number. The only valid value is

0.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the FIB and hardware.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also show ip fib

clear ip igmp groups

Clears information related to learned groups in the IGMP protocol module.

Synopsis clear ip igmp groups [A.B.C.D [interface tengigabitethernet slot/port | interface port-channel

number | interface vlan vlan_id] | interface tengigabitethernet slot/port | interface port-channel

number | interface vlan vlan_id]

Operands A.B.C.D Specifies the group address, as a subnet number in dotted decimal format

(for example, 10.0.0.1), as the allowable range of addresses included in the

multicast group.

interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid external 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

port-channel number

Specifies the interface is a port-channel. The range of valid values is from 1

through 63 for standalone mode. The range of valid values is from 1 through

6144 for VCS mode.

interface Use this keyword to specify the following interface:

vlan vlan_id Specifies which VLAN interface to display the snooping configuration related

information. The range of valid values is from 1 through 3583.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the group information in the IGMP database, including entries for

either a specific group on all interfaces or specific groups on specific interfaces.

Usage Guidelines There are no usage guidelines for this command.

Examples To clear information for all groups in the IGMP protocol:

switch#clear ip igmp groups

clear ip traffic

Clears the IP traffic statistics.

Synopsis clear ip traffic

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the IP traffic statistics.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

clear lacp

Clears the Link Aggregation Group Control Protocol (LACP) counters on a specific port-channel.

Synopsis clear lacp number counters

Operands *number* Specifies the port channel-group number. The range of valid values is from 1

through 63.

counters Clears traffic counters.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the LACP counters per specified channel-group.

Usage Guidelines There are no default configurations for this command.

Examples To clear the LACP counters for a specific port-channel:

switch#clear lacp 10 counters

See Also show lacp counter

clear lacp counters

Clears the Link Aggregation Group Control Protocol (LACP) counters on all port-channels.

Synopsis clear lacp counters

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the LACP counters for all port-channels.

Usage Guidelines There are no default configurations for this command.

Examples To clear the counters for all port-channels:

switch#clear lacp counters

See Also show lacp counter

clear IIdp neighbors

Clears the Link Layer Discovery Protocol (LLDP) neighbor information on all or specified interfaces.

Synopsis clear IIdp neighbors interface [tengigabitethernet slot/port]

Operands interface Use this keyword to specify the 10 Gbps Ethernet interface using the

tengigabitethernet operand followed by the slot or port number.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the LLDP neighbor information about the devices learned through an

interface.

Usage Guidelines If the interface operand is not specified, this command clears the LLDP neighbor information

received on all the interfaces.

Examples To clear the LLDP information for all interfaces:

switch#clear lldp neighbors

See Also show Ildp neighbors

clear IIdp statistics

Clears LLDP statistics for all interfaces or a specified interface.

Synopsis clear IIdp statistics interface [tengigabitethernet slot/port]

Operands interface Use this keyword to specify the 10 Gbps Ethernet interface using the

tengigabitethernet operand followed by the slot or port number.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear LLDP statistics for all interfaces or a specified interface.

interfaces.

Examples To clear all the LLDP statistics for all interfaces:

switch#clear lldp statistics

See Also show IIdp statistics

clear logging raslog

Clears the RASlog system messages.

Synopsis clear logging raslog [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to clear the saved RASlog messages.

Usage Guidelines There are no usage guidelines for this command.

Examples To clear the RASlog messages on the local switch:

switch# clear logging raslog

See Also logging switchid raslog console, show logging raslog, show running-config logging

clear spanning-tree counter

Clears all spanning-tree counters on the interface.

Synopsis clear spanning-tree counter [interface | port-channel number | tengigabitethernet slot/port]

Operands interface Specifies the interface on which to clear the spanning-tree counters.

port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to clear the spanning-tree counters on the interface.

Examples To clear spanning-tree counters for all interfaces:

switch#clear spanning-tree counter

To clear spanning-tree counters for a 10 Gbps Ethernet interface:

switch#clear spanning-tree counter interface tengigabitethernet 0/1

To clear spanning-tree counters for port-channel 23:

switch#clear spanning-tree counter interface port-channel 23

See Also show spanning-tree

2

clear support

Removes support data on the switch.

Synopsis clear support [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to remove support data such as core files and RAS FFDC files from the

specified switches.

Usage Guidelines There are no usage guidelines for this command.

Examples To remove the core files from the local switch:

switch#clear support

See Also copy support, show support, vcs, firmware download, firmware restore, interface management

clock set

Sets the local clock date and time.

Synopsis clock set CCYY-MM-DDTHH:MM:SS

Operands *CCYY-MM-DDTHH:MM:*SS

Specifies the local clock date and time in year, month, day, hours,

minutes, and seconds.

Description Use this command to set the local clock.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines An active NTP server, if configured, automatically updates and overrides the local clock time.

Examples To set to March 17, 2010, 15 minutes past noon:

switch# clock set 2010-03-17T12:15:00

See Also clock timezone, show clock

clock timezone

Sets the time zone based on region.

NOTE

The no clock timezone removes the time zone setting for the local clock.

Synopsis clock timezone [country / | state/]

no clock timezone

Operands country Specifies the country's time zone.

state Specifies the state's time zone.

Description Sets the local clock time zone.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines Regions include the following countries: Africa, America, Pacific, Europe, Antarctica, Asia, Australia,

Atlantic, Indian, and longitudinal city. By default, all switches are in the Greenwich Mean Time

(GMT) time zone.

Examples To set the time zone to Pacific Standard Time in the state of California in North America:

switch:clock timezone America/California

See Also show diag burninstatus, show clock

Copies a file.

Synopsis copy source_file destination_file

Operands source_file Specifies the source file as one of the following:

default-configrunning-configstartup-configThe startup configuration.

flash://filename

A file in the local flash memory.

ftp://username:password@host ip address/path

A file on a remote host. Transfer protocol is FTP.

scp://username:password@host_ip_address/path

A file on a remote host. Transfer protocol is SCP.

usb://path A file on an attached USB device.

default-configThe default configuration.running-configThe running configuration.startup-configThe startup configuration.

flash://filename

A file in the local flash memory.

ftp://username:password@host_ip_address/path

A file on a remote host. Transfer protocol is FTP.

scp://username:password@host_ip_address/path

A file on a remote host. Transfer protocol is SCP.

usb://path A file on an attached USB device.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to copy a file to another location. You can use this command to back up and

restore configuration files with various protocols.

Usage Guidelines This command is supported only on the local switch.

Examples To save the running configuration to a file:

switch# copy running-config flash://myconfig

To overwrite the startup configuration with a locally saved configuration file:

switch# copy flash://myconfig startup-config

This operation will modify your startup configuration. Do you want to continue? [Y/N]: \mathbf{Y}

To overwrite the startup configuration with a remotely archived configuration file:

```
switch# copy scp://user:password@10.10.10.10/myconfig startup-config
```

To overwrite the startup configuration with a configuration file saved on an attached USB device:

```
switch# copy usb://myconfig startup-config
```

See Also

copy running-config startup-config, delete, dir, chassis disable, show file, show support, show running-config, vcs

copy (AMPP)

Copies all properties of an existing AMPP port-profile into the current port-profile.

Synopsis copy profile-name

Operands profile-name Name of an existing port-profile from which the network policies need to be

inherited.

Defaults There are no defaults for this command.

Command Modes Port-profile mode, vlan-profile mode, qos-profile mode, fcoe-profile mode, security-profile mode

Description This command allows the user to copy all properties of an existing port-profile or a sub-profile in a

port-profile into the current port-profile. This allows the user to start with a default profile and edit

it for further customizations.

Usage Guidelines There are no usage guidelines for this command.

Examples None

copy default-config startup-config

Restores the startup configuration to the default configuration.

Synopsis copy default-config startup-config

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to copy the default configuration to the current startup configuration. This

operation effectively resets the startup configuration to factory defaults. It prompts for

confirmation because it overwrites the saved startup configuration. When the switch reboots and

comes back up, the restored default configuration is used.

Usage Guidelines This command is supported only on the local switch.

Examples To restore the default configuration:

switch# copy default-config startup-config

This operation will modify your startup configuration. Do you want to

continue? [Y/N]: Y

See Also copy, copy running-config startup-config, delete, dir, chassis disable, show support, show file,

show running-config

copy running-config startup-config

Copies the running configuration to the startup configuration.

Synopsis copy running-config startup-config

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to copy the running configuration to the startup configuration. This command

effectively saves the configuration changes you made to be applied after the switch reboots.

This command prompts for confirmation because it overwrites the startup configuration with the currently active running configuration. When the switch reboots and comes back up, the modified

configuration is used.

Usage Guidelines Use this command after you have made changes to the configuration.

The running configuration is nonpersistent across reboots.

Examples To save configuration changes:

switch# copy running-config startup-config

This operation will modify your startup configuration. Do you want to

continue? [Y/N]: Y

See Also chassis disable, copy, delete, dir, show file, show support, show running-config, vcs

copy support

Copies supportsave data.

Synopsis copy support { ftp | scp } host host_ip user username password password [all] directory directory

copy support usb [all] directory directory

copy support-interactive

Operands ftp | scp Specifies the File Transfer Protocol (ftp) or the Secure Copy Protocol (scp).

. Valid protocols are or **scp**. The values are not case-sensitive.

host *host_ip* Specifies the host IP address. Only IPv4 addresses are supported.

user *username* Specifies the user login name for the server.

password password Specifies the account password.

directory directory Specifies a fully qualified path to the directory where the supports ave output

will be stored.

usb directory directory

Specifies the directory where the supportsave output will be stored on a USB device. You must enable the USB device before you can save the data.

all Copy supports ave data for all switches in the fabric.

Defaults FTP is used if no protocol is specified.

Command Modes Privileged EXEC mode

Description Use this command to copy supports ave data to a file. You can upload supports ave data from the

local switch to an external host or you can save the data on an attached USB device.

Usage Guidelines Pagination does not apply to this command.

Examples To upload supportsave data to a remote host:

switch#copy support host 10.38.33.131 user admin password ***** directory
/home/admin/support

To upload supportsave data interactively:

 $\verb|switch#copy| \verb| support-interactive| \\$

Server Name or IP Address: 10.38.33.131

Protocol (ftp, scp): ftp

User: admin
Password: *****

Directory:/home/admin/support
VCS support [y/n]? (y): y

To save supportsave data on an attached USB device:

switch#usb on
USB storage enabled
switch#copy support usb directory support

See Also clear support, show support, vcs, firmware download, firmware restore, interface management

debug arp

Displays the ARP traffic.

Synopsis debug arp [interface interface-type interface-number] [count tx | rx]

Operands interface Displays the ARP traffic for the specified interface only.

interface-type Network interface type (TenGigabitEthernet interface, null, port-channel, or

VLAN interface).

interface-number

Layer 2 or Layer 3 interface number.

count Stops display after display count packets.

tx Counts only transmitted packets.

rx Counts only received packets.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the ARP traffic, for all interfaces or a specific interface.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

debug ip

Displays the IGMP and ICMP traffic on the switch.

Synopsis debug ip [packet [[interface interface-type interface-number] | [count tx | rx]]] | [icmp [interface

interface-type interface-number] | [count tx | rx]]| [igmp [interface interface-type

interface-number] | [all] | [group multicast-grp-address]]

Operands packet Enables IP packet debugging.

interface Displays the IP traffic for the specified interface only.

interface-type Network interface type (external TenGigabitEthernet interface, null,

port-channel, or VLAN).

interface-number

Layer 2 or Layer 3 interface number.

count Stops display after display count packets.

tx Counts only transmitted packets.

rx Counts only received packets.

icmp Displays the ICMP packets.igmp Displays the IGMP packets.

all Enables all IGMP debugging.

group Enables IGMP debugging for multicast group.

multicast-grp-address

Multicast group address.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display all IGMP or ICMP packets received or transmitted. Can be enabled

globally, per interface, or on a multicast group.

Usage Guidelines There are no usage guidelines for this command.

Examples None

debug ip igmp

Displays all IGMP information.

Synopsis debug ip igmp [all | group [A.B.C.D [interface tengigabitethernet slot/port] port-channel number |

vlan vlan_id]]]

Operands all Displays all values.

group A.B.C.D Specifies the group address, as a subnet number in dotted decimal format

(for example, 10.0.0.1), as the allowable range of addresses included in the

multicast group.

interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

port-channel number

Specifies the interface is a port-channel. The range of valid values is from 1 through 63 for standalone mode. The range of valid values is from 1 through

6144 for VCS mode.

vlan vlan_id Specifies which VLAN interface to display the snooping configuration related

information. The range of valid values is from 1 through 3583.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Displays all of the IGMP packets received and sent, and IGMP-host related events.

Usage Guidelines There are no usage guidelines for this command.

Examples None

debug lacp

Enables debugging for the Link Aggregation Control Protocol (LACP).

Synopsis debug lacp [all | cli | event | nsm | pdu [rx [all | interface tengigabitethernet slot/port] | tx [all |

interface tengigabitethernet slot/port]] | sync | timer | trace level number]

no debug lacp

Operands all Turns on all debugging.

cli Turns on command line interface debugging.

event Turns on event debugging.

nsm Turns on Network Services Module (NSM) debugging.

pdu Turns on PDU debugging.

rx all Turns on debugging for received LACP packets on all interfaces.

rx interface Turns on debugging for received LACP packets on the specified

interface.

interface tengigabitethernet

Specifies the 10 Gbps Ethernet interface.

slot Specifies the slot number.

port Specifies the port number.

tx all Turns on debugging for transmitted LACP packets on all interfaces.

tx interface Turns on debugging for transmitted LACP packets on the specified interface.

interface tengigabitethernet

Specifies the 10 Gbps Ethernet interface.

slot Specifies the slot number.

port Specifies the port number.

sync Turns on debugging for LACP sync transitions.

timer Turns on debugging for LACP timers.

trace level number Specifies the trace level number. The range of valid values is from 1 through

7.

Defaults By default, debugging is not turned on.

Command Modes Privileged EXEC mode

Description Use this command to enable debugging for Link Aggregation Control Protocol (LACP). Use the **no**

debug lacp command to disable debugging.

Usage Guidelines To display debug outputs on a specific cmsh session, use the terminal monitor command.

Examples To enable debugging of LACP PDUs for transmitted and received packets on all interfaces:

switch#debug lacp pdu tx all
switch#debug lacp pdu rx all

switch#show debug lacp
LACP rx debugging is on
LACP tx debugging is on

See Also show debug lacp

debug lldp packet

Enables debugging for Link Layer Discovery Protocol (LLDP).

Synopsis debug lldp packet [all | interface tengigabitethernet s/ot/port [both]] | [detail [both | rx | tx]]

no debug lldp packet [all | interface tengigabitethernet slot/port]

Operands all Turns on LLDP packet debugging on all interfaces.

interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

both Turns on debugging for both transmit and receive packets.

detail Turns on debugging with detailed information.

both Turns on detailed debugging for both transmit and receive packets.

Turns on detailed debugging for only received LLDP packets.Turns on detailed debugging for only transmitted LLDP packets.

Defaults By default, debugging is not turned on.

Command Modes Privileged EXEC mode

Description Use this command to enable debugging for Link Layer Discovery Protocol (LLDP). Use the **no debug**

Ildp packet command to disable debugging.

Usage Guidelines To display debugging outputs on a particular cmsh session, use the **terminal monitor** command.

Examples To enable debugging of LLDP for both received and transmitted packets on 10 Gbps Ethernet

interface 0/1:

switch#debug lldp packet interface tengigabitethernet 0/1 both

switch#show debug lldp
LLDP debugging status:

Interface te0/1 : Transmit Receive

See Also show debug lldp

debug spanning-tree

Enables debugging for the Spanning Tree Protocol.

Synopsis debug spanning-tree [all | bpdu [rx | tx [all | interface port-channel number | tengigabitethernet

slot/port]]

no debug spanning-tree [all | bpdu [rx | tx [all | interface port-channel number |

tengigabitethernet slot/port]]

Operands all Turns on spanning tree packet debugging on all interfaces.

bpdu Turns on Bridge Protocol Data Unit debugging.

rx Turns on debugging for only received spanning-tree packets.

tx Turns on debugging for only transmitted spanning-tree packets.

interface Use this keyword to specify any of the following interfaces:

port-channel number

Specifies the port-channel interface. The range of valid values is from 1

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults By default debugging is not turned on.

Command Modes Privileged EXEC mode

Description Use this command to enable debugging for the Spanning Tree Protocol. Use the **no**

debugspanning-tree command to disable debugging.

Usage Guidelines To display debugging outputs on a particular cmsh session, use the terminal monitor command.

Examples To enable debugging of spanning-tree for both Rx and Tx on 10 Gbps Ethernet interface 0/1:

switch#show debug spanning-tree

MSTP debugging status:

Spanning-tree rx debugging is off Te 0/1 rx is on Spanning-tree tx debugging is off Te 0/1 tx is on

See Also show debug spanning-tree

delete

Deletes a file from the flash memory.

Synopsis delete file

Operands file Specifies the name of the file to be deleted.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to delete a user-generated file from the switch. This operation is final; there is

no mechanism to restore the file.

Usage Guidelines This command is supported only on the local switch.

System configuration files cannot be deleted. If you try to delete a system configuration file, an

appropriate message is displayed.

Examples To delete a configuration file:

See Also

copy, copy running-config startup-config, dir, chassis disable, show file, show running-config, show support, vcs

deny (extended ACLs)

Configures a MAC address rule to drop traffic based on the source and destination MAC addresses.

Synopsis deny [any | host MAC_ACL | MAC_ACL | [any | host MAC_ACL | MAC_ACL] [EtherType | arp | fcoe |

ipv4] [count]

 $\textbf{no deny} \ [\textbf{any} \ | \ \textbf{host} \ \textit{MAC_ACL} \ | \ \textit{MAC_ACL} \] \ [\textbf{E}ther\textit{Type} \ | \ \textbf{arp} \ | \ \textbf{arp} \ | \ \textbf{ACL} \]$

fcoe | ipv4]

Operands any Specifies any source MAC address.

host MAC_ACL Specifies the source host MAC address for which to set deny conditions. Use

the format HHHH.HHHH.

MAC_ACL Specifies the destination host MAC address for which to set deny conditions.

Use the format HHHH.HHHHH.

any Specifies any destination MAC address.

host MAC_ACL Specifies the source host address for which to set deny conditions. Use the

format HHHH.HHHH.

MAC_ACL Specifies the destination host address for which to set deny conditions. Use

the format HHHH.HHHH.

EtherType Specifies the protocol number for which to set the deny conditions. The

range of valid values is from 1536 through 65535.

arp Specifies to deny the Address Resolution Protocol (0x0806).

fcoe Specifies to deny the Fibre Channel over Ethernet Protocol (0x8906).

ipv4 Specifies to deny the IPv4 protocol (0x0800).

count Enables counting of the packets matching the rule.

Defaults By default, no MAC ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to configure rules to match and drop traffic based on the source and

destination MAC addresses and the protocol type. You can also enable counters for a specific rule. There are 255 ACL counters supported per port group. Use the **no deny** command to remove a rule

from the MAC ACL.

Usage Guidelines The first set of [any | host MAC_ACL | MAC_ACL] parameters is specific to the source MAC

address. The second set of [any | host MAC_ACL | MAC_ACL] parameters is specific to the

destination MAC address.

Examples To create a rule in a MAC extended ACL to drop IPv4 traffic from the source MAC address

0022.3333.4444 to the destination MAC address 0022.3333.5555 and to enable the counting

of packets:

switch(conf-macl-ext)#deny 0022.3333.4444 0022.3333.5555 ipv4 count

2

To delete a rule from a MAC extended ACL:

switch(conf-macl-ext)#no deny 0022.3333.4444 0022.3333.5555 ipv4

See Also

mac access-list extended, mac access-list standard, permit (extended ACLs), permit (standard ACLs)

deny (standard ACLs)

Configures a MAC address rule to drop traffic based on the source MAC address.

Synopsis deny [MAC_ACL | any] [count]

no deny [MAC_ACL | any]

Operands MAC_ACL Specifies the source host MAC address for which to set deny conditions. Use

the format HHHH.HHHHH.

any Specifies any source MAC address.

count Enables counting of the packets matching the rule.

Defaults By default, no MAC ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to configure rules to match and to drop traffic based on the source MAC

address. You can also enable counters for a specific rule. There are 255 ACL counters supported

per port group. Use the **no deny** command to remove a rule from the MAC ACL.

Usage Guidelines There are no usage guidelines for this command.

Examples To create a rule in a MAC standard ACL to drop traffic from the source MAC address

0022.3333.4444 and to enable the counting of packets:

switch(conf-macl-std)#deny 0022.3333.4444 count

To delete a rule from a MAC standard ACL:

switch(conf-macl-std) #no deny 0022.3333.4444

See Also mac access-list extended, mac access-list standard, permit (extended ACLs), permit (standard

ACLs)

description (interfaces)

Specifies a string that contains the description of the interface.

Synopsis description line

no description

Operands line Specifies characters describing the interface. The maximum number of

characters is 64.

Defaults There are no default configurations for this command.

Command Modes Interface configuration mode

Description Use this command to specify a string that contains the description of the interface. Use the no

description command to remove the description.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the string describing internal tengigabitethernet interface 0/1:

switch(conf-if-te-0/1)#description converged_101

description (LLDP)

Specifies a string that contains the description of LLDP.

Synopsis description line

no description

Operands *line* Characters describing LLDP.

Defaults There are no default configurations for this command.

Command Modes Protocol LLDP configuration mode

Description Use this command to specify a string that contains the description of the LLDP. Use the **no**

description command to remove the description.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the strings describing LLDP:

switch(conf-lldp)#description Brocade-LLDP

description (Port Mirroring)

Specifies a string that contains the description of the Port Mirroring session.

Synopsis description line

no description

Operands line Specifies characters describing the interface. The maximum number of

characters is 64.

Defaults None

Command Modes Monitor session mode

Description This is a label that describes the Port Mirroring session, displayed in the running-config file.

Usage Guidelines Use this command to specify a string that contains the description of the Port Mirroring session.

Use the no description command to remove the description string.

Examples To set the string describing monitor session 1:

sw0(config)#monitor session 1

sw0(config-mon-sess-1)#description server group 1 switch-cmsh

See Also monitor session

diag burninerrclear

Clears the errors that are stored in the nonvolatile storage on the slot during the burn-in process.

Synopsis diag burninerrclear slotNum

Operands slotNum Specifies the number of the slot on which errors that are stored in

nonvolatile storage are cleared.

Description Use this command to clear errors that are stored in the nonvolatile storage on the slot during the

burn-in process.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To clear the burn-in errors from the specified slot:

switch# diag burninerrclear slotNum

See Also diag clearerror, show diag burninerrshow, show diag burninstatus

2

68

diag clearerror

Clears the diagnostics failure status.

Synopsis diag clearerror

Operands None

Description Use this command to clear the diagnostics failure status.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To clear the diagnostic failure status:

switch# diag clearerror

See Also diag burninerrclear, show diag burninerrshow, show diag burninstatus

diag portledtest

Runs various action modes on the port LEDs and validates the functionality.

Synopsis diag portledtest [npass count] [action number]

Operands npass count Specifies the number of times to perform this test. The default value is 10.

> action number Specifies the LED color:

> > 0 — Cycle all port LEDs.

1 — Turn port status LED off.

2 - Turn port status LED amber.

Description Use this command to exercise the user port LEDs.

Defaults The default npass value is 10.

By default, all the ports are tested in a switch.

The default action is cycle_all

Command Modes Privileged EXEC mode (with the chassis disabled in offline mode)

Usage Guidelines There are no usage guidelines for this command.

> Examples To run various action modes on the LEDs and validate the functionality:

> > switch# diag portledtest -npass 20 -ports 10 -action cycle_all

To display all possible port LED actions:

switch# diag portledtest action?

Possible completions:

blink_amber Blink Port status LED amber blink_green Blink Port status LED green

cycle_all Cycle all Port LEDs

status_amber Turn Port status LED amber status_green Turn Port status LED green

turn_off Turn Port status LED off

See Also diag portloopbacktest, diag post

diag portloopbacktest

Sends frames between various ASICs on the switch and validates the ASIC functionality.

Synopsis diag portloopbacktest [nframes count] [lbmode mode] [spdmode mode]

Operands nframes count Specifies the number of frames to send.

Ibmode mode Specifies the loopback point for the test. By default, the port loopback test

uses internal loopback.

spdmode mode Specifies the speed mode for the test. This parameter controls the speed at

which each port operates during the test.

Description Use this command to send frames between various ASICS on the switch and to validate ASIC

functionality.

Defaults The default number of frames (**nframes**) is 0

The default loopback mode (Ibmode) is 2

The speed mode (spdmode) depends on the platform. On a 10 Gbps port, the default speed mode

is 10.

Command Modes Privileged EXEC mode (with the chassis disabled, in offline mode)

Usage Guidelines There are no usage guidelines for this command.

Examples To send frames between various ASICs on the switch and validate the functionality:

switch# diag portloopbacktest nframes 20 lbmode 2 spdmode 8

1bmode:

Mode Description

1 Port Loopback (external loopback plugs)

2 Internal loopback located externally to ASIC (serial line)

5 Internal loopback located internally to ASIC (parallel line)

spdmode:

Mode Description

1 Runs test at 1 Gbps 10 Runs test at 10 Gbps

nframes: integer number (default=10)

See Also diag portledtest, diag post

diag post

Enables and disables the power-on self-test (POST).

Synopsis diag post [switchid] enable

no diag post

Operands switchid Specifies the switch ID on which POST is run.

enable Enables the power-on self-test on the specified switch.

Description Use this command to enable or disable POST during bootup.

Defaults By default, POST is enabled.

Command Modes Global configuration mode

Usage Guidelines The **no** option disables the POST.

Examples To enable POST:

switch(config)# diag post enable

To disable POST:

switch(config)# no diag post

See Also show diag post results

2

diag setcycle

Configures all the parameters required for the system verification test.

Synopsis diag setcycle [default {Y | N}]

Operands default Y | N Sets the default values.

Specify **Y** to set the default values. Specify **N** to set custom values.

Description Sets the user-defined parameters for running a system verification test.

Defaults The following settings are the default values:

number_of_runs—1

• min_lb_mode-2

tbr_passes or turborramtest number of passes—1

plb_nframes or portloopbacktest number of frames—20

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To configure all the parameters required to run during system verification:

switch(config) # diag setcycle default Y

See Also show diag setcycle

diag system verification

Runs a combination of various hardware diagnostic tests.

Synopsis diag system verification [short]

Operands *short* Sets the burn-in parameters that control the number of frames to one.

Description Use this command to execute a combination of various system hardware diagnostic tests.

Defaults If short is not specified, all the burn-in parameters that control the number of frames are run.

Command Modes Privileged EXEC mode (with the chassis disabled in offline mode)

Usage Guidelines The primary use for this command is software regression testing, or a quick validation that all

hardware is operational.

Examples To run various tests, such as the memory and portloopback tests, with various combinations:

switch# diag systemverification

2

diag turboramtest

Performs a turbo static RAM (SRAM) test of the ASIC chips.

Synopsis diag turboramtest [passcnt count]

Operands passent count Specifies the number of test repetitions. By default, the test runs once.

Description Use this command to run a turbo static RAM test of the ASIC chips.

Defaults By default, the pass count (passcnt) is one.

Command Modes Privileged EXEC mode (with the chassis disabled in offline mode).

Usage Guidelines There are no usage guidelines for this command.

Examples To run turbo static RAM tests on various ASICs on the switch:

switch# diag turboramtest -passcnt 10

dir

Lists the contents of the switch flash memory.

Synopsis dir

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to list the files in the flash memory.

Usage Guidelines This command is supported only on the local switch.

Examples To list the contents of the flash memory:

```
switch# dir
total 24
drwxr-xr-x 2 root
                        sys
                                      4096 Feb 13 00:39 .
drwxr-xr-x 3 root root
-rwxr-xr-x 1 root sys
-rwxr-xr-x 1 root sys
                                      4096 Jan 1 1970 ..
                                       417 Oct 12 2010 myconfig.vcs
                                       417 Oct 12 2010 defaultconfig.novcs
-rwxr-xr-x 1 root
                                       697 Oct 12 2010 defaultconfig.vcs
                        sys
                                      6800 Feb 13 00:37 startup-config
-rw-r--r-- 1 root
                        root
switch#
```

See Also

copy, copy running-config startup-config, delete, chassis disable, show file, show running-config, show support, vcs

2

dot1x authentication

Enables dot1x on a port.

Synopsis dot1x authentication

no dot1x authentication

Operands None

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description Use this command to enable dot1x on a port. Use the **no dot1x authentication** command to

disable dot1x on the port and remove the configuration from 802.1X management.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable dot1x on a port:

switch(config)#interface tengigabitethernet 0/16
switch(conf-if-te-0/16)#dot1x authentication

dot1x enable

Enables 802.1X authentication globally.

Synopsis dot1x enable

no dot1x enable

Operands None

Defaults By default, authentication is disabled globally.

Command Modes Global configuration mode

Description Use this command to globally enable 802.1X authentication. Use the **no dot1x enable** command

to disable 802.1X authentication globally.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable 802.1X authentication globally:

switch(config)#dot1x enable

2

dot1x port-control

Controls the authorization of a port state.

Synopsis dot1x port-control [auto | force-authorized | force-unauthorized]

no dot1x port-control

Operands auto Enables authentication on a port.

forced-authorized Forces a port to remain in an authorized state.

force-unauthorized

Forces a port to remain in an unauthorized state.

Defaults The default port state is auto.

Command Modes Interface configuration mode

Description Use this command to control the authorization of a port state. Use the **no dot1x port-control**

command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable the port state to auto:

switch(config)#interface tengigabitethernet 0/16
switch(conf-if-te-0/16)#dot1x port-control auto

dot1x quiet-period

Sets the number of seconds that a switch remains quiet between a failed authentication and an

attempt to retry authentication.

Synopsis dot1x quiet-period interval seconds

no dot1x quiet-period

Operands interval seconds Specifies the time in seconds between attempts at authentication. The

range of valid values is from 1 through 65535.

Defaults The default time is 60 seconds.

Command Modes Interface configuration mode

Description Use this command to set the time in seconds after which a switch attempts to perform

authentication after a failed authentication. Use the **no dot1x quiet-period** command to return to the default setting. When a switch cannot authenticate a client, the switch remains idle for a

quiet-period interval of time, then attempts the operation again.

Usage Guidelines Changing the quiet-period interval time to a number lower than the default can result in a faster

response time.

Examples To change the interval time to 200 seconds:

 $\verb|switch(config)#interface tengigable thernet 0/16|\\$

switch(conf-if-te-0/16)#dot1x quiet-period interval 200

dot1x reauthenticate interface

Initiates reauthentication on a specified interface.

Synopsis dot1x reauthenticate interface [tengigabitethernet slot/port]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to initiate the reauthentication on a specified interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To initiate reauthentication on interface tengigabitethernet 0/16:

switch#dot1x reauthenticate interface tengigabitethernet 0/16

dot1x reauthentication

Enables reauthentication on a port.

Synopsis dot1x reauthentication

Operands None

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description Use this command to enable reauthentication on a port.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable reauthentication on a port:

switch(config)#interface tengigabitethernet 0/16
switch(conf-if-te-0/16)#dot1x reauthentication

dot1x reauthMax

Sets the maximum number of times that a port attempts to reauthenticate.

Synopsis dot1x reauthMax number

no dot1x reauthMax

Operands number Specifies the maximum number of reauthentication attempts before the port

goes to the unauthorized state. The range of valid values is from 1 through

10.

Defaults The default number of times that a port attempts authentication is 2.

Command Modes Interface configuration mode

> Description Use this command to set the maximum number of times that a port attempts to reauthenticate

> > before a port changes to the unauthorized state. Use the no dot1x reauthMax command to return

to the default setting.

Usage Guidelines There are no usage guidelines for this command.

> **Examples** To set the maximum number of reauthentication attempts to 5:

> > switch(config)#interface tengigabitethernet 0/16 switch(conf-if-te-0/16))#dot1x reauthMax 5

To set the reauthentication maximum to the default value:

switch(config)#interface tengigabitethernet 0/16

switch(conf-if-te-0/16)#no dot1x reauthMax

dot1x timeout re-authperiod

Sets the number of seconds between reauthorization attempts.

Synopsis dot1x timeout re-authperiod seconds

Operands seconds Specifies the seconds between reauthorization attempts. The range of valid

values is from 1 through 4294967295.

Defaults The default time is 3600 seconds.

Command Modes Interface configuration mode

Description Use this command to set the number of seconds between reauthorization attempts.

Usage Guidelines There are no usage guidelines for this command.

Examples To set 25 seconds as the amount of time between reauthorization attempts:

switch(config)#interface tengigabitethernet 0/16
switch(conf-if-te-0/16)#dot1x timeout re-authperiod 25

dot1x timeout server-timeout

Sets the authentication sever response timeout.

Synopsis dot1x timeout server-timeout seconds

Operands seconds Specifies the number of seconds that a switch waits for the response from

the authentication server. The range of valid values is from 1 through

65535.

Defaults The default timeout is 30 seconds.

Command Modes Interface configuration mode

Description Use this command to set the authentication sever response timeout.

Usage Guidelines There are no usage guidelines for this command.

Examples To set 40 seconds as the switch-to-authentication server transmission time:

switch(config)#interface tengigabitethernet 0/16

switch(conf-if-te-0/16)#dot1x timeout server-timeout 40

dot1x timeout supp-timeout

Sets the time in seconds that a switch waits for a response to an Extensible Authentication

Protocol (EAP) request frame from the client before resending the request.

Synopsis dot1x timeout supp-timeout seconds

Operands seconds Specifies the number of seconds that the switch waits for a response to the

EAP frame. The range of valid values is from 1 through 65535.

Defaults The default timeout is 30 seconds.

Command Modes Interface configuration mode

Description Use this command to specify the EAP response timeout.

Usage Guidelines There are no usage guidelines for this command.

Examples To set 45 seconds as the switch-to-client retransmission time for the EAP request frame:

switch(config)#interface tengigabitethernet 0/16
switch(conf-if-te-0/16)#dot1x timeout supp-timeout 40

dot1x timeout tx-period

Sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) request or identity frame from the client before retransmitting the request.

Synopsis dot1x timeout tx-period seconds

Operands seconds Specifies the time in seconds between successive request ID attempts. The

range of valid values is from 1 through 65535.

Defaults The default timeout is 30 seconds.

Command Modes Interface configuration mode

Description Use this command to set the interval between successive attempts to request an ID (EAP ID Req).

Usage Guidelines There are no usage guidelines for this command.

Examples To set 34 as the number of seconds to wait for a response to an EAP-request or identity frame from

the client before retransmitting the request:

switch(config)#interface tengigabitethernet 0/16
switch(conf-if-te-0/16)#dot1x timeout tx-period 34

dpod

Manages Dynamic Ports on Demand (POD) assignments.

Synopsis dpod slot/port { reserve | release }

Operands slot Specifies the slot number.

port Specifies the port number.

reserve Reserves a POD assignment for a port that is currently not able to come

online but is expected to be viable in the future. A port license assignment that is reserved will be associated with the first port set that has a vacancy.

release Removes a port from the port set to which it is currently assigned.

Defaults None

Command Modes Global configuration mode.

Description Use this command to manage Dynamic POD assignments.

A port POD assignment can only be released if the port is currently offline. Use the **shutdown**

command to take the port offline.

Usage Guidelines Do not release a port unless you plan to disconnect the optical link or disable the port persistently.

If the link (server or optical) is left in a state where the port could be brought online, the Dynamic

POD mechanism will detect this unassigned port and attempt to reassign it to a port set.

Examples To reserve a POD assignment on the local switch:

switch(config)# dpod 0/10 reserve
switch(config-dpod-0/10)# exit
switch(config)# dpod 0/11 reserve
switch0(config-dpod-0/11)# exit

To remove a port from a POD port set:

switch(config)# dpod 0/10 release
switch(config-dpod-0/10)# exit
switch(config)# dpod 0/11 release
switch(config-dpod-0/11)# exit

See Also show dpod, show running-config dpod

2 end

end

Returns to the Privileged EXEC command mode from all configuration modes.

Synopsis end

Operands None

Defaults There are no default configurations for this command.

Command Modes All configuration modes

Description Use this command to return to the Privileged EXEC command mode from any command mode.

Usage Guidelines There are no usage guidelines for this command.

Examples To return to the Privileged EXEC mode from interface configuration mode:

switch(config)#interface tengigabitethernet 0/0

switch(conf-if-te-0/0)#end

switch#

See Also exit

error-disable-timeout enable

Enables the timer to bring the interface out of the error-disabled state.

Synopsis error-disable-timeout enable

Operands None

Defaults There are no default configurations for this command.

Command Modes Protocol Spanning Tree mode

Description Use this command to enable the timer to bring the interface out of the disabled state.

Usage Guidelines When the Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) guard disables a port,

the port remains in the disabled state unless the port is enabled manually. This command allows

you to enable the interface from the disabled state.

Examples To bring the interface out of the disabled state:

switch(conf-rstp)#error-disable-timeout enable

See Also error-disable-timeout interval

error-disable-timeout interval

Synopsis error-disable-timeout interval seconds

Operands seconds Specifies the range of time in seconds for the interface to time out. The

range of valid values is from 10 through 1000000.

Defaults The default is 300 seconds. The timeout feature is disabled.

Command Modes Protocol Spanning Tree mode

Description Use this command to set the interface to time out when an error occurs.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the timeout value to 10 seconds:

switch(conf-rstp)#error-disable-timeout interval 10

See Also error-disable-timeout enable

exit

Exits the current mode and returns to the previous mode.

Synopsis exit

Operands None

Defaults There are no default configurations for this command.

Command Modes All command modes

Description Use this command to exit the current mode, and return to the previous mode. When used in EXEC

and Privileged EXEC modes, the exit command terminates the session.

Usage Guidelines There are no usage guidelines for this command.

Examples To exit the Interface configuration mode, and return to the global configuration mode:

 $\verb|switch(config)#interface tengigabitethernet 0/1|\\$

switch(conf-if-te-0/1)#exit

switch(config)#exit

See Also end

fabric isl enable

Enables and disables the administration and operational state of an inter-switch link (ISL).

Synopsis fabric isl enable

no fabric isl enable

Operands None

Description Use this command to set the state of an ISL. If the port is connected to another switch when this

command is issued, the fabric may reconfigure.

Defaults By default, ISL ports are enabled persistently.

Command Modes Global configuration mode

Usage Guidelines No edge port configuration is allowed on an ISL.

Examples To enable the administration and operational state of an ISL:

switch(config-TenGigabitEthernet-1/0/18)# fabric isl enable

See Also diag setcycle, show diag burninstatus, show diag burninstatus, vcs

fabric route multicast

Sets the multicast priority for the local RBridge in the fabric.

Synopsis fabric route multicast rbridgeld id priority priority

Operands rbridgeld Specifies the ID of the routing bridge.

id Specifies the RBridge identifier.

priority Sets a priority (default is 0). The highest priority overrides the lowest RBridge

ID and becomes the root.

priority Specifies the priority number of the RBridge.

Description Use this command to set the multicast priority for the local RBridge in the fabric. The multicast

routing information indicates all ports that are members of the multicast distribution tree: ports

that are able to send and receive multicast frames.

Defaults The default priority is 0.

Command Modes Privileged EXEC mode

Usage Guidelines The root of the tree is auto-selected as the switch with the lowest RBridge ID.

Examples To change an RBridge multicast priority:

switch(config)# fabric route multicast rbridgeId 7 priority 67

See Also show fabric route multicast, show fabric route topology, show running-config fabric route mcast

fabric trunk enable

Enables and disables trunking on a port.

Synopsis fabric trunk enable

no fabric trunk enable

Operands None

Description Use this command to enable or disable trunking on a port. When the command is executed to

update the trunking configuration, the port to which the configuration applies is disabled and subsequently re-enabled with the new trunking configuration. Traffic through the ports may be

temporarily disrupted.

NOTE

Enabling trunking requires an ISL trunking license. You can disable trunking without a license.

Defaults Fabric trunking is enabled by default.

Command Modes Global Configuration mode.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable a port for trunking:

 $switch (\texttt{config-TenGigabitEthernet-1/0/18}) \# \ \textbf{fabric trunk enable}$

See Also show fabric trunk

fabric-map

Enables the Fabric-Map sub-mode.

Synopsis fabric-map default

Operands None

Defaults There are no defaults for this command.

Command Modes FCoE configuration mode

Description This command enables the FCoE map sub-mode. An FCOE fabric-map is equivalent to an FC

Virtual-Fabric.

Usage Guidelines The only map name allowed is "default."

You must be in the feature configuration mode for FCoE for this command to function.

Examples switch(config)#fcoe

switch(config-fcoe)#fabric-map default

switch(config-fcoe-fabric-map)#

See Also fcoe

2 fastboot

fastboot

Reboots the control processor (CP), bypassing the power-on self-tests (POST).

Synopsis fastboot

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to perform a "cold reboot" (power off and restart) of the control processor,

by passing POST when the system comes back up. By passing POST can reduce boot time $\,$

significantly. If POST was previously disabled, then fastboot is the same as reload.

Usage Guidelines The fastboot operation is disruptive, and the command prompts for confirmation before executing.

When you reboot a switch connected to a fabric, all traffic to and from that switch stops. All ports

on that switch remain inactive until the switch comes back online.

Examples To perform a cold reboot on the switch:

switch#fastboot

Are you sure you want to fastboot the switch [y/n]?: y

See Also reload

fcmap

Configures the FCMAP for an FCoE fabric-map.

Synopsis fcmap hh:hh:hh

Operands *hh:hh:hh* A valid FPMA FCMAP value.

Defaults The default value is 0E:FC:00.

Command Modes FCoE fabric-map configuration mode

Description Use this command to configure the FPMA FCMAP value for the FCoE fabric-map.

Usage Guidelines You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Examples switch#configuration terminal

switch(config)#fcoe

switch(config-fcoe)#fabric-map default

switch(config-fcoe-fabric-map)#fcmap 0E:FC:00

See Also fcoe, fabric-map

2 fcoe

fcoe

Enables the FCoE configuration mode.

Synopsis fcoe

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Enables the FCoE configuration mode, allowing the configuration of various FCoE options.

Usage Guidelines There are no usage guidelines for this command.

Examples switch(config)#fcoe

switch(config-fcoe)#

See Also fcoe, fabric-map

fcoeport map

Provisions a port with the default FCoE map.

Synopsis fcoeport default

Operands None

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description This command configures a specific tengigabit Ethernet port to be an FCoE port, with the assigned

map name "default."

Examples switch(config-if-te-0/1)#fcoeport default

fcoe-profile (AMPP)

Activates the FCoE profile configuration mode.

Synopsis fcoe-profile

Operands None

Defaults There are no defaults for this command.

Command Modes Port-profile mode

Description This command activates the FCoE profile configuration mode for AMPP. This mode allows

configuration of FCoE attributes of a port-profile.

Usage Guidelines There are no usage guidelines for this command.

Examples switch(config)#port-profile default

switch(conf-pp)#fcoe-profile

firmware commit

Commits the switch firmware.

Synopsis firmware commit

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description

Use this command to manually commit a firmware download. This command copies an updated firmware image to the secondary partition and commits both partitions of the Control Processor to the firmware upgrade. Wait until the switch has rebooted and you have confirmed that the new image is operational.

By default, **firmware download** updates the secondary partition only. When **firmware download** completes successfully and the Control Processor is rebooted, the system switches partitions, so the primary partition (with the old firmware) becomes the secondary partition, and the secondary partition (with the new firmware) becomes the primary partition.

By default, **firmware download** automatically commits the firmware after the switch reboots. If you decide to disable autocommit mode when running **firmware download**, you must execute one of the following two commands after you reboot the switch:

- **firmware commit** Copies the primary partition (with the new firmware) to the secondary partition and commits the new firmware to both partitions of the Control Processor.
- **firmware restore** Copies the secondary partition (with the old firmware) to the primary partition and restores the original firmware version.

Usage Guidelines

This command is supported on the local switch only. The **firmware download** command must have been run with the **nocommit** option for the **firmware commit** operation to succeed.

Examples To commit the firmware:

```
switch#firmware commit
Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
...........
FirmwareCommit completes successfully.
```

See Also firmware download, firmware restore, interface management, show version

firmware download

Downloads the switch firmware.

Synopsis firmware download interactive

ftp [nocommit] [noreboot] host host_ip_address user username password password
directory directory [file file_name]

scp [nocommit] [noreboot] host host_ip_address user username password password
directory directory [file file_name]

usb directory directory

firmware download [nocommit] [noreboot] { ftp | scp } host host_ip_address user username password password directory [file file_name]

firmware download usb directory directory

Operands interactive Runs firmware download in interactive mode. You are prompted for input.

ftp | scp Valid protocols are ftp (File Transfer Protocol) or scp (Secure Copy). The

values are not case sensitive.

nocommit Disables autocommit mode. When autocommit mode is disabled, you must

execute the **firmware commit** command manually to propagate the downloaded image to both partitions of the Control Processor.

noreboot Disables autoreboot mode. When autoreboot mode is disabled, you must

reboot the switch manually. If autocommit mode was disabled, you must perform a manual **firmware commit** operation after the switch comes back

up.

host host_ip_address

Specifies the host IP address. Only IPv4 addresses are supported.

user *username* Specifies the user login name for the server.

password password Specifies the account password.

directory directory Specifies a fully qualified path to the directory where the firmware is located.

file filename Specifies the firmware .plist file. This operand is optional; if unspecified, the

default file, release.plist, is used.

usb directory directory

Downloads the firmware from an attached USB device. You must enable the USB device prior to the firmware download with the **usb on** command. Firmware must be stored under the firmware directory in the USB file system.

Defaults By default, the **firmware download** command performs a full install, autoreboot, and autocommit.

Command Modes Privileged EXEC mode

Description Use this command to download switch firmware from an external host or from an attached USB

device. You can run this command interactively or provide the parameters on the command line.

The systems supported by this firmware have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions so the secondary partition becomes the primary partition.

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partition.

Usage Guidelines

This command supports local firmware upgrade only.

This command does not support pagination.

If **firmware download** is interrupted due to an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples To download firmware interactively:

```
switch#firmware download interactive
Server Name or IP Address: 10.38.33.131
File Name: nos2.0.0
Protocol (ftp, scp): ftp
User: admin
Password:******
Do Auto-Commit after Reboot [Y]:y
Reboot system after download [Y]:y
This command will cause a cold/disruptive reboot and will require that
existing telnet, secure telnet or SSH sessions be restarted.
Do you want to continue (Y/N) [Y]: y
Server IP: 10.38.33.131, Protocol IPv4
Checking system settings for firmware download...
Server IP: 10.38.33.131, Protocol IPv4
You are running 'firmware download' with auto-reboot and auto-commit enabled.
After the firmware is downloaded the system will reboot and commit firmware
automatically.
2010/09/23-14:31:44, [SULB-1001], 64858, WARNING, VDX6720-24,
Firmwaredownload command has started.
2010/09/23-14:31:44, [SULB-1036], 64859, INFO, VDX6720-24, The current
Version: NOS v2.0.0.0_bld16
dir
                ldconfig
                glibc
                [output truncated]
```

To download firmware from an attached USB device using the command line:

```
switch# firmware download usb directory \
/usb/usbstorage/brocade/firmware/NOS_v2.0.0
```

See Also vcs, firmware restore, interface management, show version

firmware restore

Restores the previous firmware image.

Synopsis firmware restore

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to restore the former active firmware image. This command can only be run if

autocommit mode was disabled during the firmware download. After a firmware download and a reboot (with autocommit mode disabled), the downloaded firmware becomes active. If you decide

you do not want to commit the firmware upgrade, use the firmware restore command.

This command reboots the system and reactivates the previous firmware. After reboot, both

primary and secondary partitions restore the previous firmware image.

Usage Guidelines This command is supported on the local switch only.

The firmware download command must have been run with the nocommit option for the firmware

restore operation to succeed.

This command requires a reboot after a firmware download.

Examples To restore the previous firmware:

```
switch#firmware restore
```

Restore old image to be active ...

Restore both primary and secondary image after reboot.

The system is going down for reboot NOW !!

Broadcast message from root (ttyS0) Fri Oct 26 23:48:54 2001...

Doing firmwarecommit now.

Please wait ..

See Also vcs, firmware download, interface management, show version

forward-delay

Specifies the time an interface spends in each of the listening and learning states.

Synopsis forward-delay seconds vlan_id

no forward-delay

Operands seconds Specifies the range of time in seconds that an interface spends in the

Spanning Tree Protocol (STP) learning and listening states. The range of valid

values is from 4 through 30.

vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults The default is 15 seconds.

Command Modes Protocol Spanning Tree mode

Description Use this command to specify how long the listening and learning states last before the interface

begins the forwarding of all spanning-tree instances. Use the **no forward-delay** command to return to the default settings.

STP interface states:

• Listening - The interface processes the Bridge Protocol Data Units (BPDUs) and awaits possible new information that might cause it to return to the blocking state.

 Learning - The interface does not yet forward frames (packets), instead it learns source addresses from frames received and adds them to the filtering database (switching database).

• Forwarding - An interface receiving and sending data, normal operation. STP still monitors incoming BPDUs that can indicate it should return to the blocking state to prevent a loop.

Blocking - An interface that can cause a switching loop, no user data is sent or received, but it
might go to the forwarding state if the other links in use fail and the STP determines that the
interface may transition to the forwarding state. BPDU data continues to be received in the
blocking state.

Usage Guidelines

When you change the spanning-tree forward-delay time, it affects all spanning-tree instances. When configuring the forward-delay, the following relationship should be kept:

2*(forward-delay - 1)>=max-age>=2*(hello-time + 1)

Examples To configure the forward-delay time to 18 seconds:

switch(conf-mstp)#forward-delay 18

See Also hello-time, max-age

2 hello

hello

Sets the Hello transmit interval.

Synopsis hello seconds

no hello

Operands seconds The range of valid values is from 4 through 180 seconds.

Defaults The default is 30 seconds.

Command Modes Protocol LLDP configuration mode

Description Use this command to set the interval between LLDP hello messages. Use the **no hello** command to

return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the time interval to 10 seconds between the transmissions:

switch#configure terminal
switch (config) #protocol 1ldp
switch(conf-lldp)#hello 10

hello-time

Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent on an interface.

Synopsis hello-time seconds vlan_id

no hello-time

Operands seconds Specifies the time range in seconds for the interval between the hello BPDUs

sent on an interface. The range of valid values is from 1 through 10.

vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults The default is 2 seconds.

Command Modes Protocol Spanning Tree mode

Description Use this command to configure the spanning-tree bridge hello time, which determines how often

the device broadcasts hello messages to other devices. Use the no hello-time command to return

to the default settings.

Usage Guidelines When configuring the hello-time, the max-age command setting must be greater than the

hello-time setting. The following relationship should be kept:

2*(forward-delay - 1)>=max-age>=2*(hello-time + 1)

Examples To configure spanning-tree bridge hello time to 5 seconds:

switch(conf-stp)#hello-time 5

See Also forward-delay, max-age

instance

Maps a VLAN to a Multiple Spanning Tree Protocol (MSTP) instance.

Synopsis instance instance_id [vlan vlan_id | priority priority_id]

no instance

Operands instance_id Specifies the MSTP instance. The range of valid values is from 1 through 15.

vlan vlan_id Specifies the VLAN to map an MSTP instance. The range of valid values is

from 1 through 3583.

priority priority_id

Specifies the priority for the specified instance. The range of valid values is from 0 through 61440. The priority values can be set only in increments of

4096.

Defaults The default priority value is 32768.

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to map a VLAN to an MTSP instance. You can group a set of VLANs to an

instance. This command can be used only after the VLAN is defined. Use the no instance command

to unmap the VLAN from the MSTP instance.

Usage Guidelines The following rules apply:

VLANs must be created before mapping to instances.

VLAN instance mapping is removed from the configuration if the underlying VLANs are

deleted.

Examples To map a VLAN to an MTSP instance:

switch(conf-mstp)#instance 1 vlan 2, 3
switch(conf-mstp)#instance 2 vlan 4-6
switch(conf-mstp)#instance 1 priority 4096

See Also show spanning-tree

interface

Enters the interface configuration mode to configure an interface.

Synopsis interface [port-channel number | tengigabitethernet slot/port [shut] | vlan vlan_id]

no interface [port-channel number | vlan vlan_id]

Operands interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

shut When this command is issued, if either the fabric ISL or VF port is online, a

link shutdown is sent to that internal port.

port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

3583.

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to create or enter the interface configuration mode to configure an interface.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also show interface, interface vlan

2

interface fcoe

Logs all users out and then sends a link shutdown event to the switch driver.

Synopsis interface fcoe [shut | no shut]

Operands shut Logs out users.

no shut Cancels shutdown event and allows logins again.

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description Internally, the FC switch infrastructure only sees a link as up on a VF port when an FCoE FLOGI is

accepted. It will see link as down if all the devices log out, or if the physical interface is link down. The **interface fcoe shut** command logs all users out and then sends a link shutdown event to the switch driver. No further logins are allowed while the port is configured in this manner. The

interface fcoe no shut command allows the port to accept logins again.

Usage Guidelines There are no usage guidelines for this command.

Examples None

interface management

Configures the management interface.

Synopsis interface management switchID/0

ip { address { ip_address/prefix_len | dhcp } | gateway-address gateway_address }
no ip { address { ip_address/prefix_len | dhcp } | gateway-address gateway_address }
ipv6 address { ipv6_address/prefix_len | autoconfig }
no ipv6 address { ipv6_address/prefix_len | autoconfig }
speed { 10 | 100 | auto }
no speed

Operands switchID/O

Specifies the switch management interface to be configured as the *switchID* followed by a slash (/) and the port number. The port number for the management port is always 0.

ip address

Configures the management IP address in IPv4 format. The **no** option removes the configuration.

ipv4_address/prefix_len

Specified the IP address in IPv4 format using a prefix.

dhcp

Enables dynamic host configuration protocol (DHCP) on the

management port. The no option disables DHCP.

ip gateway-address gateway_address

Configures an IPv4 gateway address. The **no** option removes the configuration.

ipv6 address

Configures the management IP address in IPv6 format using a prefix. The **no** option removes the configuration.

ipv6_address/prefix_len

Specified the IP address in IPv6 format using a prefix.

autoconfig

Enables IPv6 stateless auto-configuration.

speed

Sets the speed for the management interface. The **no** option removes the configuration. Valid speed values are:

10 10 Mbps Full Duplex100 100 Mbps Full Duplexauto Auto negotiation (default)

Defaults

There is no default IPv4 static address.

There is no default IPv4 gateway address.

DHCP is disabled by default.

There is no default IPv6 static address.

IPv6 stateless auto-configuration is disabled by default.

The default speed setting is auto negotiation.

2

Command Modes Global configuration mode

Description Use this command to configure the management interface. This command supports IP addresses

in IPv6 and IPv4 format.

Usage Guidelines Setting a static IPv4 address and DHCP are mutually exclusive. If DHCP is enabled, you must

disable DHCP before you can configure a static IPv4 address. Use the no option to disable DHCP or

remove the static IPv4 address.

A staticIPv6 address and stateless auto-configuration can co-exist.

Examples To configure a management interface with an IPv4 IP address:

switch(config)# interface management 1/0
switch(config-Management-1/0)# no ip address dhcp
switch(config-Management-1/0)# ip address 10.24.85.81/20
switch(config-Management-1/0)# ip gateway-address 10.24.80.1

To configure a management interface with an IPv6 IP address:

switch(config)# interface management 1/0
switch(config-Management-1/0)# ipv6 address \
fd00:60:69bc:832:e61f:13ff:fe67:4b94/64

To set the interface to 100 Mbps Full Duplex

switch(config-Management-2/0)# speed 100

See Also show interface management, show running-config interface management

interface vlan

Configures a VLAN interface.

Synopsis interface vlan vlan_id

no interface vlan vlan_id

Operands *vlan_id* Specifies the VLAN interface to configure. The range of valid values is from 1

through 4094.

Defaults VLAN 1 is predefined on the switch.

Command Modes Global configuration mode

Description Use this command to configure a VLAN interface. Use the **no interface vlan** vlan_id command to

delete a VLAN interface.

Usage Guidelines All of the ports on the switch are a part of the default VLAN 1.

Make sure your converged mode interface is not configured to classify untagged packets to the same VLAN as the incoming VLAN-tagged packets. By configuring a converged interface to classify untagged packets (by using classifiers or the default port *vlan_id*) to the same VLAN as VLAN-tagged packets coming into the interface, the FCoE hardware sends out untagged packets to

the CNA. These packets may be dropped, disrupting communications.

Examples To create a VLAN with ID 56:

switch(config)#interface vlan 56
switch-cmsh(conf-if-vl-56)#

See Also switchport, fcmap, shutdown (STP)

2

ip address

Configures an IP address.

Synopsis ip address ip-address/mask [secondary]

no ip address ip-address/mask [secondary]

Operands ip-address IP address.

mask Mask for the associated IP subnet. Only integers from from 1 to 31 are

supported. Dotted-decimal is not supported.

secondary Specifies that the configured address is a secondary IP address. If this

keyword is omitted, the configured address is the primary IP address.

Defaults There are no default configurations for this command.

Command Modes Interface configuration mode

Description Use this command to configure an IP address.

Usage Guidelines Use **no ip address** to remove the IP address.

This command is supported on VLANs, LAGs and external TenGigabitEthernet interfaces.

When the secondary parameter is not specified, this command overwrites the primary IP address.

When the secondary parameter is specified, this command adds a new IP address to the interface.

The secondary address cannot be configured in the absence of a primary IP.

Examples None

ip igmp last-member-query-interval

Sets the last member query interval.

Synopsis ip igmp last-member-query-interval milliseconds

Operands milliseconds Response time in milliseconds. The range of valid values is from 1000

through 25500 milliseconds.

Defaults Default value is 1000 milliseconds.

Command Modes Privileged EXEC mode

Description The last member query interval is the amount of time in seconds that the IGMP router waits to

receive a response to a group query message.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

ip igmp query-interval

Sets the query interval.

Synopsis ip igmp query-interval seconds

Operands seconds Response time in seconds. The range of valid values is from 1 through

18000 seconds.

Defaults Default value is 125 seconds.

Command Modes Privileged EXEC mode

Description The query interval is the amount of time in seconds between IGMP query messages sent by the

witch.

Usage Guidelines There are no usage guidelines for this command.

Examples None

ip igmp query-max-response-time

Sets the maximum response time for IGMP queries.

Synopsis ip igmp query-max-response-time seconds

Operands seconds Response time in seconds. The range of valid values is from 1 through 25

seconds.

Defaults Default value is 10 seconds.

Command Modes Privileged EXEC mode

Description When a host receives the query packet, it starts counting to a random value, less that the

maximum response time. When this timer expires, the switch replies with a report, provided that

no other host has responded yet.

Usage Guidelines There are no usage guidelines for this command.

Examples None

ip igmp snooping enable (global version)

Enables the Internet Group Management Protocol (IGMP) snooping for all VLAN interfaces.

Synopsis ip igmp snooping enable

no ip igmp snooping enable

Operands None

Defaults IGMP snooping is globally disabled.

Command Modes Global configuration mode

Description Use this command to enable or disable the Internet Group Management Protocol (IGMP) snooping

globally. Use the no ip igmp snooping enable command to return to the default setting.

Usage Guidelines This command performs IGMP snooping at the interface level.

Examples To enable IGMP globally:

switch(config)#ip igmp snooping enable

See Also show ip igmp snooping, ip igmp snooping enable (VLAN version)

ip igmp snooping enable (VLAN version)

Enables the Internet Group Management Protocol (IGMP) snooping for a specific VLAN interface.

Synopsis ip igmp snooping enable

no ip igmp snooping enable

Operands None

Defaults When snooping is enabled globally, IGMP snooping enabled on all VLAN interfaces.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable the Internet Group Management Protocol (IGMP) snooping

on a specific VLAN interface.

Usage Guidelines This command performs IGMP snooping at the VLAN interface level.

Examples To enable IGMP for a specific VLAN interface, enter Interface VLAN mode and execute the following

command:

switch#ip igmp snooping enable

See Also show ip igmp snooping, ip igmp snooping enable (global version)

ip igmp snooping fast-leave

Enables snooping fast-leave.

Synopsis ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Operands None

Defaults This mode is disabled by default.

Command Modes Global configuration mode

Description IGMP snooping fast-leave processing allows the removal of an interface from the forwarding-table

without sending out group-specific queries to the interface.

Usage Guidelines Use **no ip igmp snooping fast-leave** to disable this function.

Examples None

ip igmp snooping mrouter

Configures a VLAN port member to be a multicast router interface.

Synopsis ip igmp snooping mrouter interface [tengigabitethernet slot/port] | [interface port-channel

number]

no ip igmp snooping mrouter

Operands interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

port-channel number

Specifies the interface is a port-channel. The range of valid values is from 1 through 63 for standalone mode. The range of valid values is from 1 through

6144 for VCS mode.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to configure a VLAN port member to be a multi-router port.

Use the no ip igmp snooping mrouter version of this command to return to the default setting.

Examples To configure a VLAN port member to be a multicast router interface.

switch#ip igmp snooping mrouter interface tengigabitethernet 0/1

See Also show ip igmp snooping

ip igmp snooping mrouter-timeout

Configures the mrouter timeout value for IGMP snooping.

Synopsis ip igmp snooping mrouter-timeout seconds

Operands seconds Timeout time in seconds. Valid range is from 1 to 60000 seconds.

Defaults Default value is 300 seconds.

Command Modes Privileged EXEC mode

Description This command sets the timeout range for when multicast router ports are automatically learned.

Usage Guidelines There are no usage guidelines for this command.

Examples None

ip igmp snooping querier enable

Activates or deactivates the IGMP snooping querier functionality for the VLAN.

Synopsis ip igmp snooping querier enable

no ip igmp snooping querier enable

Operands None

Defaults This feature is not enabled by default.

Command Modes Privileged EXEC mode

Description Use this command to activate or deactivate the IGMP snooping querier functionality for the VLAN.

Usage Guidelines Use **no ip igmp snooping querier enable** to disable this command.

Examples To enable the IGMP snooping querier feature:

switch(conf-if-vl-1)#ip igmp snooping querier enable

See Also show ip igmp snooping

ip igmp static-group

Configures the static group membership entries.

Synopsis ip igmp static-group A.B.C.D interface [tengigabitethernet slot/port] | [port-channel number]

no ip igmp static-group

Operands A.B.C.D Specifies the group address, as a subnet number in dotted decimal format

(for example, 10.0.0.1), as the allowable range of addresses included in the

multicast group.

interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

port-channel number

Specifies the interface is a port-channel. The range of valid values is from 1

through 63 for standalone mode. The range of valid values is from 1 through

6144 for VCS mode.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Using **ip igmp static-group**, packets to the group are fast-switched out of the interface, providing

that the packets were received on the correct reverse path forwarding (RPF) interface. Static group

membership entries are automatically added to the IGMP cache and mroute table.

Use the no ip igmp static-group version of this command to return to the default setting.

Examples None

keep-alive timeout (fabric-map)

Enables or disables the keep-alive timeout.

Synopsis keep-alive timeout

no keep-alive timeout

Operands None

Defaults There are no defaults for this command.

Command Modes FCoE fabric-map configuration mode

Description This command enables the keep-alive timeout.

Usage Guidelines Use **no keep-alive timeout** to disable the keep-alive timeout.

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Examples None

See Also fcoe, fabric-map

12traceroute

The **I2traceroute** command sends a simple traceroute from the source MAC address to the destination MAC address. This command is not supported in the standalone mode.

Synopsis I2traceroute

Operands None

Description Use this command to send a plain layer 2 traceroute, hop by hop, from the switch that learned the

source MAC address to the switch that learned the destination MAC address. The IP parameters included in the **I2traceroute** command allows generating frames with similar properties as the one

generated from a connected device, thus traversing the same path through the fabric.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines Configuration results depend on the configuration options you select. The following describes the fields that display when you first enter the **!2traceroute** command:

- Source mac address—Specifies the source MAC address. This field is mandatory. The MAC address must be a valid MAC address that exists in the mac-address-table.
- Destination mac address—Specifies the destination MAC address. This field is mandatory. The MAC address must be a valid MAC address that exists in the mac-address-table.
- Vlan [1-3583]—Specifies the VLAN number. The valid VLAN number range is from 1 through 3583.
- Extended commands [Y/N]—Enter Y to enable extended commands, which include protocol type (IP or FCoE), source IP address, destination IP address, IP protocol type (TCP or UDP), source port number, and destination port number.
- Protocol Type [IP | FCOE]—Specifies the protocol type. You must select either IP or FCOE.
- Source IP address—Specifies the source IP address.
- Destination IP address—Specifies the destination IP address.
- IP Protocol Type [TCP|UDP]—Specifies the IP protocol type. You must select TCP or UDP.
 - Transmission Control Protocol (TCP) is a connection-oriented protocol, which means that it requires handshaking to set up end-to-end communications.
 - User Datagram Protocol (UDP) is a message-based connectionless protocol.
 Communication occurs by transmitting information in one direction, from the source to the destination, without verifying the readiness of the receiver.
- Source port number [0-65535]—Specifies the source port number. The valid port range is from 0 through 65535.
- Dest port number [0-65535]—Specifies the destination port number. The valid port range is from 0 through 65535.

Examples Case-1: Example of extended commands, IP protocol type, and TCP as the IP Protocol Type.

NOTE

Although IP and FCoE appear as choices in the Protocol Type field, IP is the only supported type.

```
switch# 12traceroute
Source mac address : 11:11:11:11:11
Expected format[11:11:11:11:11:11]
Source mac address : 11:11:11:11:11:11
Destination mac address : 11:11:11:11:11:11
Vlan [1-3583] : 1
Extended commands [Y/N]? : Y
Protocol Type [IP/FCOE] : IP
Source IP address : 192.85.1.2
Destination IP address : 192.0.2.2
IP Protocol Type [TCP/UDP] : TCP
Source port number [0-65535]: 58
Dest port number [0-65535] : 67
```

The following output indicates that RBridge 4 responded first, followed by RBridge 3 and RBridge 2. RBridge 4 responded in 1020 microseconds, RBridge 3 in 5939 microseconds, and 2 in 9629 microseconds.

RBRIDGEID	RoundTrip Time (u-sec)
4	1020
3	5939
2	9629

Case-2: Example of extended commands, IP protocol type, and UDP as the IP Protocol Type.

SWitch# 12traceroute

```
Source mac address : 11:11:11:11:11:11

Destination mac address : 11:11:11:11:11:11

Vlan [1-3583] : 1

Extended commands [Y/N]? : Y

Protocol Type [IP/FCOE] : IP

Source IP address : 192.85.1.2

Destination IP address : 192.0.2.2

IP Protocol Type [TCP/UDP] : UDP

Source port number [0-65535] : 58

Dest port number [0-65535] : 67
```

The following output indicates that RBridge 4 responded first, followed by RBridge 3 and RBridge 2. RBridge 4 responded in 1110 microseconds, RBridge 3 in 5239 microseconds, and 2 in 9920 microseconds.

RBRIDGEID	RoundTrip Time (u-sec)
4	1110
3	5239
2	9920

Case-3: Example of no extended commands.

```
switch# 12traceroute
Source mac address : 0e:fc:00:ff:03:00
Destination mac address : 0e:fc:00:ff:03:01
Vlan [1-3583] : 1
Extended commands [Y/N]? : N
```

2

The following output indicates that RBridge 4 responded first, followed by RBridge 3 and RBridge 2. RBridge 4 responded in 2091 microseconds, RBridge 3 in 4667 microseconds, and 2 in 9624 microseconds.

RBRIDGEID RoundTrip Time (u-sec)

- 4 2091
- 3 4667
- 2 9624

lacp system-priority

Sets the Link Aggregation Control Protocol (LACP) system priority.

Synopsis lacp system-priority value

no lacp system-priority

Operands value Specifies the value of the LACP system priority. The range of valid values is

from 1 through 65535.

Defaults The default system-priority value is 32768.

Command Modes Global configuration mode

Description Use this command to set the system priority of a local system. This determines which system is

responsible for resolving conflicts in the choice of aggregation groups. Use the **no lacp**

system-priority command to reset the system priority to the default value.

Usage Guidelines Lower numerical values have higher priorities.

Examples To set the LACP system-priority to 68:

switch(config)#lacp system-priority 68

To clear the configured LACP system-priority:

switch(config)#no lacp system-priority

2

lacp timeout

Sets the timeout value used by LACP to exchange packets on an interface.

Synopsis lacp timeout [long | short]

no lacp timeout

Operands timeout Specifies the number of seconds before invalidating a received Link

Aggregation Control Protocol (LACP) data unit (DU).

long Specifies a long timeout value.short Specifies a short timeout value.

Defaults By default, the short timeout value is 3 seconds for Brocade trunks. For standard trunks, the long

timeout value is 90 seconds.

Command Modes Interface configuration mode

Description Use this command to set the short timeout value for Brocade trunks or to set the long timeout

value for standard trunks. Use the no lacp timeout command to return to the default value.

Usage Guidelines If the LACP_timeout bit (encoded in Actor_State and Partner_State fields) is set to 1, the short

timeout takes effect; if set to 0 (zero), the long timeout takes effect.

Examples To set the LACP short timeout value to 5 seconds:

switch(conf-if-te-0/1)#lacp timeout short 5

license add

Adds a license key to a switch.

Synopsis license add licstr licenseString [switchId switchID]

Operands licstr license String Specifies the license string to be added to the switch. The license string must

be enclosed in double quotation marks.

switchId switchID Executes the command on the remote switch specified by the switch ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to add a license key to a switch.

Usage Guidelines Depending on the feature being added, you must reboot the switch or disable and re-enable the

chassis or port for this command to take effect. Follow the instructions in the command output.

Examples To add a license on the local switch:

```
switch# license add licstr "*B
r84pNrtHKdrZujmwAUT63GOrXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:qWx3hH2:9RsMv3BHfeCRFM2qj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6qpx7,73t#"
```

Adding license [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvwl:fUjANF av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]

To add a license on a remote switch specified by its switch ID:

```
switch# license add licstr "*B
r84pNrtHKdrZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvwl:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#
" switchId 2
Adding license for switchId 2 [*B
r84pNrtHKdrZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvwl:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#
```

See Also license remove, show license, show license id

]

license remove

Removes a license key from a switch.

Synopsis license remove licstr { *license*String | *feature* } [**switchId** switchID]

Operands licetr licenseString Removes the specified license string and associated feature. The license

string must be enclosed in double quotation marks.

licstr feature Removes the license string associated with the specified feature from the

license database of the local switch. The feature name must be enclosed in

double quotation marks.

switchId switchID Executes the command on the remote switch specified by the switch ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to remove a license from a switch or to deactivate a temporary license that

cannot be removed.

Usage Guidelines You cannot display the license string once you install it. If you do not remember the string, use the

feature name to remove the license.

Depending on the feature being removed you must reboot the switch or disable and re-enable the

chassis or port for this command to take effect.

This command deactivates but does not permanently remove time-based trial licenses.

Examples To remove a license string from a remote switch specified by its switch ID:

```
switch# license remove licstr "*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvwl:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#
" switchId 2
```

```
Removing license for switchId 2 [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

To remove a license based on the feature name from a remote switch specified by its switch ID:

```
switch# license remove licstr "FCOE_BASE" switchId 2
removing license feature name [FCOE_BASE]
```

See Also license add, show license, show license id

line vty exec-timeout

Sets the CLI session timeout.

Synopsis line vty exec-timeout timeout

no line vty exec-timeout

Operands timeout Specifies the CLI session timeout period in minutes. Valid values are from 0

through 136. The default session timeout is 10 minutes. The no option

disables auto-logout by deleting the timeout value.

Defaults The default timeout value is 10 minutes.

Command Modes Global configuration mode

Description Use this command to specify the amount of time a CLI session can be idle before it logs you out.

Use the **no** option to disable auto-logout.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the terminal timeout to 60 minutes:

switch(config)# line vty exec-timeout 60

See Also terminal length

IIdp dcbx-version

Specifies which version of the Data Center Bridging Exchange (DCBX) protocol to use.

Synopsis IIdp dcbx-version [auto | cee | pre-cee]

Operands auto Specifies to auto adjust the DCBX protocol version to accommodate the

difference when a switch interacts with different vendors using a different

version of the DCBX protocol.

cee Specifies to use the Converged Enhanced Ethernet (CEE) DCBX version.

pre-cee Specifies to use the standard DCBX version, which is the version released

prior to the CEE DCBX release.

Defaults The default is auto.

Command Modes Interface configuration mode

Description Use this command to specify which version of the DCBX protocol to use.

Usage Guidelines There are no usage guidelines for this command.

Examples To specify which DCBX version to use:

switch(conf-if-te-0/1)#lldp dcbx-version cee

Ildp disable

Disables LLDP on the interface.

Synopsis Ildp disable

no lldp disable

Operands None

Defaults By default, LLDP is enabled at both the global and interface levels.

Command Modes Interface configuration mode

Description Use this command to disable LLDP on the interface. Use the **no lldp disable** command to enable

LLDP on the interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To disable LLDP on the interface.

switch(conf-if-te-0/1)#lldp disable

IIdp iscsi-priority

Configures the priority that will be advertised in the DCBX iSCSI TLV.

Synopsis IIdp iscsi-priority value

no IIdp iscsi-priority

Operands value Specifies the priority value. The range of valid values is from 0 through 7.

Defaults The default value is 4.

Command Modes Interface configuration mode

Description The iSCSI priority setting is used to configure the priority that will be advertised in the DCBX iSCSI

TLV. The no lldp iscsi-priority command returns to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the priorities on which iSCSI traffic is allowed:

switch(conf-if-te-0/1)#lldp iscsi-priority 5

See Also protocol IIdp

Ildp profile

Applies a Link Layer Discovery Protocol (LLDP) profile on an interface.

Synopsis IIdp profile *name*

no lldp profile

Operands name Specifies the profile name.

Defaults If the parameters are not defined in the profile, the default values are used.

Command Modes Interface configuration mode

Description Use this command to apply a Link Layer Discovery Protocol (LLDP) profile on an interface. Use the

no lldp profile command to delete the profile from the interface.

Usage Guidelines You must use the profile command to create an LLDP profile before you can apply the profile to the

interface. Only one LLDP profile can exist at any time for a particular interface. When this command is not present, the parameters defined in the global LLDP configuration are used.

Examples To apply an LLDP profile on an interface:

switch(conf-if-te-0/1)#lldp profile test

See Also protocol IIdp

logging switchid raslog console

Sets the severity levels for the RASlog console.

Synopsis logging switchid switchID raslog console severity

no logging switchid switchID raslog console

Operands switchid switchID Specifies the switch ID.

severity Specifies the minimum severity level of the message to pass through the

filter. Valid values consist of one of the following: INFO, WARNING, ERROR, or

CRITICAL. Input values are case-sensitive.

Defaults The default severity level is INFO.

Command Modes Global configuration mode

Description Use this command to set the severity levels for the RASlog console. Use the no logging switchid

switchID raslog console command to reset the severity to the default value (INFO).

Usage Guidelines There are no usage guidelines for this command.

Examples To set the RASlog severity levels on switch 2:

switch(config)# logging switchid 2 raslog console WARNING

To reset the RASlog severity levels to the default value.

switch(config)# no logging switchid 2 raslog console

See Also clear logging raslog, logging switchid raslog console, show running-config logging

logging syslog-server

Configures a switch to forward system messages to specified servers.

Synopsis logging syslog-server *ip_address*

no logging syslog-server ip_address

Operands ip_address Specifies the IP address of the syslog server in IPv4 format.

Defaults None

Command Modes Global configuration mode

Description Use this command to configure a switch to forward all error log entries to the syslog daemon

(syslogd) of one or more specified servers. Up to four servers are supported. Use the no logging

syslog-server command to remove the specified configured IP address.

Usage Guidelines You can configure up to four syslog servers. You must execute the command for each server.

Examples To configure a server to which system messages are sent:

switch(config)# logging syslog-server 192.168.163.233

To add a second IP address to the existing syslog server configuration:

switch(config)# logging syslog-server 192.168.163.234

To remove a configured syslog server:

switch(config)# no logging logging syslog-server 192.168.163.233

See Also show running-config logging syslog-server

mac access-group

Applies rules specified in a MAC ACL to traffic entering an interface.

Synopsis mac access-group name [in]

no mac access-group name

Operands name Specifies the name of the standard or extended MAC access list.

in Specifies to filter inbound packets only.

Defaults There are no access lists applied to the interface.

Command Modes Interface configuration mode

Description Use this command to apply a MAC ACL to a Layer 2 or a VLAN interface. You create the MAC ACL by

using the mac access-list global configuration command. Use the no mac access-group command

to remove the MAC ACL from the interface.

Usage Guidelines You can assign one MAC ACL (standard or extended) to an interface.

When a packet is received on an interface with a MAC ACL applied, the switch checks the rules in the ACL. If any of the rules match, the switch permits or drops the packet, according to the rule. If

the rest of all AOI desired materials the secretary permits of dispersions dispersions, described

the specified ACL does not exist, the switch permits all the packets.

Examples To apply a MAC ACL named macacl2 on an interface:

switch(conf-if)#mac access-group macacl2 in

To remove a MAC ACL named macacl2 from an interface:

switch(conf-if)#no mac access-group macacl2

See Also mac access-list standard, mac access-list extended

mac access-list extended

Creates and assigns a name to the extended MAC access list.

Synopsis mac access-list extended name

no mac access-list extended name

Operands name Assigns a name to the MAC extended access list. The maximum character

limit is 64.

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to create an extended MAC access list. If the ACL is already created, this

command puts the switch in the extended MAC access-list configuration mode. Use the ${f no}$ ${f mac}$

access-list extended command to remove the access list.

Extended ACLs allow you to filter traffic based on the following:

Source MAC address

Destination MAC address

EtherType

You can apply named MAC extended ACLs to VLANs and to Layer 2 interfaces.

Usage Guidelines Standard and extended MAC ACLs cannot share the same name.

Examples To create a MAC extended ACL named mac1:

```
switch(config)#mac access-list extended mac1
switch(conf-macl-ext)#
```

To delete a MAC extended ACL named mac1:

switch(config)#no mac access-list extended mac1

See Also deny (extended ACLs), deny (standard ACLs), permit (extended ACLs), permit (standard ACLs)

mac access-list standard

Creates and assigns a name to the standard MAC access list.

Synopsis mac access-list standard name

no mac access-list standard name

Operands name Assigns a name to the MAC standard access list. The maximum character

limit is 64.

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to create a standard MAC access list. If ACL is already created, this command

puts the switch in the standard MAC access-list configuration mode. Use the **no mac access-list**

standard command to remove the access list.

Standard ACLs allow you to filter traffic based on the source MAC address. You can apply named

MAC standard ACLs to VLANs and to Layer 2 interfaces.

Usage Guidelines Standard and extended MAC ACLs cannot share the same name.

Examples To create a MAC standard ACL named mac1:

switch(config)#mac access-list standard mac1

switch(conf-macl-std)#

To delete a MAC standard ACL named mac1:

switch(config)#no mac access-list standard mac1

See Also deny (extended ACLs), deny (standard ACLs), permit (extended ACLs), permit (standard ACLs)

mac-address-reduction

Activates the MAC address reduction feature.

Synopsis mac-address-reduction [enable | disable]

Operands enable Enables MAC address reduction.

disable Disables MAC address reduction.

Defaults There are no default configurations for this command.

Command Modes PVST or RPVST command mode

Description Use this command to enable or disable the MAC address reduction feature.

Usage Guidelines There are no usage guidelines for this command.

Examples None

mac-address-table

Use this command to set the aging time or to add static addresses to the MAC address table.

Synopsis

mac-address-table [aging-time seconds | static mac-addr forward [port-channel number |

tengigabitethernet slot/port | vlan vlan_id]

no mac-address-table

Operands

aging-time seconds

Specifies the time in seconds that a learned MAC address will persist after the last update. If the aging time is set to zero (0), it means that aging is disabled. For standalone mode, the range of valid values is from 10 through 100000. For VCS mode, the range of valid values is from 60 through

100000.

static mac-addr

Specifies the Media Access Control (MAC) address (unicast or multicast) to add to the address table. Packets with this destination address received in

the specified VLAN are forwarded to the specified interface.

forward

Forwards the MAC address to the interface.

port-channel number

Specifies the port-channel number. The range of valid values is from $\ensuremath{\mathtt{1}}$

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

vian vian_id Specifies the VLAN number. The range of valid values is from 1 through

3583.

Defaults

The default aging time is 300 seconds.

Command Modes

Global configuration mode

Description

Use this command to set the aging time or to add static addresses to the MAC address table.

Usage Guidelines

The vian keyword is mandatory because the switch only supports independent VLAN learning (IVL).

Use the no mac-address-table version of this command to reset the values.

Examples

To add the static address 0011.2222.3333 to the MAC address table with a packet received on

VLAN 100:

switch(config)#mac-address-table static 0011.2222.3333 forward
tengigabitethernet 0/1 vlan 100

To set the aging time to 10 minutes:

switch(config) #mac-address-table aging-time 600

See Also

show mac-address-table

map

Enables the map configuration mode.

Synopsis map default

Operands None

Defaults There are no defaults for this command.

Command Modes FCoE configuration mode

Description Use this command to configure the FCoE map.

Usage Guidelines You must be in the feature configuration mode for FCoE for this command to function.

Examples switch(config)#fcoe

switch(config-fcoe)#map default
switch(config-fcoe-map-default)#

See Also fcoe

2

max-age

Sets the interval time in seconds between messages that the spanning tree receives from the

interface.

Synopsis max-age seconds vlan_id

no max-age

Operands seconds Configures the Spanning tree Protocol interface maximum age. The range of

valid values is from 6 through 40.

vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults The default is 20 seconds.

Command Modes Protocol Spanning Tree mode

Description Use this command to control the maximum length of time that passes before an interface saves its

configuration Bridge Protocol Data Unit (BPDU) information. Use the **no max-age** command to

return to the default configuration.

Usage Guidelines When configuring the maximum age, the max-age command setting must be greater than the

hello-time command setting. The following relationship should be kept:

2*(forward-delay - 1)>=max-age>=2*(hello-time + 1)

Examples To configure the maximum-age to 10 seconds:

 $\verb|switch(conf-rstp)| \# \verb|max-age 10| \\$

See Also hello-time, forward-delay

max-hops

Configures the maximum number of hops for a Bridge Protocol Data Unit (BPDU) in an MSTP

region.

Synopsis max-hops hop_count

no max-hops

Operands hop_count Specifies the maximum number of hops for which the BPDU will be valid. The

range of valid values is from 1 through 40.

Defaults The default is 20 hops.

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to configure the maximum number of hops for a BPDU in an MSTP region. This

parameter is used by all the instances of the MSTP. Use the no max-hops command to return to

the default value.

Usage Guidelines Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely on the

interface. When you change the number of hops, it affects all spanning-tree instances.

Examples To set the number of maximum hops to 25 for all MSTPs:

switch(config)#protocol spanning-tree mstp

switch(conf-mstp)#max-hops 25

See Also show spanning-tree mst brief

2

minimum-links

Sets the minimum bandwidth.

Synopsis minimum-links num-of-links

no minimum-links

Operands *num-of-links* Number of links. The range of valid values is from 1 through 16.

Defaults The default number of links is 1.

Command Modes Port channel interface configuration mode

Description Use this command to allow a port-channel to operate at a certain minimum bandwidth all the time.

If the bandwidth of the port-channel drops below that minimum number, then the port-channel is

declared operationally DOWN even though it has operationally UP members.

Usage Guidelines Use **no minimum-links** to disable this command.

Examples None

mode

Sets the LLDP mode on the switch.

Synopsis mode tx | rx

no mode

Operands tx Specifies to enable only the transmit mode.

rx Specifies to enable only the receive mode.

Defaults Both transmit and receive modes are enabled.

Command Modes Protocol LLDP configuration mode

Description Use this command to set the LLDP mode on the switch. Use the **no mode** command to return to

the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable only the transmit mode:

switch(conf-lldp)#mode tx

See Also show IIdp interface

monitor session

Enables a Port Mirroring session for monitoring traffic.

Synopsis monitor session session_number [source tengigabitethernet slot/port | destination

tengigabitethernet slot/port | direction rx | tx | both]

no monitor session session_number

Operands session_number Specifies a session identification number. The range of valid values is from 0

through 65535.

source Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid external 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

destination Use this keyword to specify the following interfaces:

tengigabitethernet

Specifies a valid external 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

direction rx Specifies to monitor the receiving traffic.

direction tx Specifies to monitor the transmitting traffic

direction both Specifies to monitor transmitting and receiving traffic.

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to enable a session for monitoring traffic. Use the **no monitor session** session

number command to delete the port mirroring connection or session.

Usage Guidelines An internal or external 10 Gbps Ethernet port can be used as the source port. Only external 10

Gbps Ethernet ports can be used as the destination port.

The source and destination ports must be in the same port-group on the Brocade VDX 6720-60.

Examples To enable session 40 for monitoring traffic:

 $\verb|switch(config)| \# monitor session 40 source tengigabite thernet 0/1 destination|\\$

tengigabitethernet 0/15 direction both

mtu

Specifies the MTU on the interface.

Synopsis mtu size

Operands size Specifies the size of the maximum transmission unit (MTU) of an interface.

The allowed MTU size is from 1522 to 9208 bytes.

Defaults By default, all 10 Gbps Ethernet interfaces use a default MTU of 2500 bytes.

Command Modes Interface configuration mode

Description Use this command to specify the MTU on the interface.

Usage Guidelines Creating MTUs under VLAN interfaces is not valid.

Examples None

2

multiplier

Sets the number of consecutive misses of hello messages before LLDP declares the neighbor as

dead.

Synopsis multiplier value

no multiplier

Operands value Specifies a multiplier value to use. The range of valid values is from 1

through 10.

Defaults The default multiplier value is 4.

Command Modes Protocol LLDP configuration mode

Description Use this command to set the number of consecutive misses of hello messages before LLDP

declares the neighbor as dead. Use the no multiplier command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the number of consecutive misses:

switch(conf-lldp)#multiplier 2

See Also hello

ntp server

Specifies or adds an NTP server IP address.

Synopsis ntp server *ip-address*

no ntp server

Operands ip-address Specifies the IPv4 IP address (dot-decimal notation) or the IPv6 IP address

(hexadecimal colon-separated notation).

Description Use this command to add an NTP server IPv4 or IPv6 address to a list of server IP addresses.

Defaults The NTP server list is LOCL (no NTP server configured).

Command Modes Global configuration mode

Usage Guidelines At least one IP address entered in the list must be a reachable, configured NTP server or the

request will fail. The maximum number of NTP servers allowed is 5.

Examples To specify an NTP server:

switch(config)# ntp server 192.168.10.1

To remove an NTP server from the current list:

switch(config)# no ntp server 192.168.10.1

See Also show diag burninstatus

password-attributes

Configures global password attributes.

Synopsis password-attributes [min-length minlen] [max-retry retry] [character-restriction [upper] [lower]]

[numeric num] [special-char char]

no password-attributes [character-restriction [upper 0-32] [lower 0-32]

Operands min-length The minimum password length.

minlen Specifies the minimum length of the password. Set the minimum from 8

through 32 characters. The default is 8 characters.

max-retry The number of times a user can specify an incorrect password during login

before the account is locked.

retry Specifies the number of failed password logins before the user is locked out.

The lockout threshold can range from 0 through 16. The default value is 0.

character-restriction The minimum number of uppercase and lowercase alphabetic characters

that must occur in the password.

upper Specifies the minimum number of uppercase alphabetic characters that

must occur in the password. The default is zero, which means there is no

restriction of uppercase characters.

lower Specifies the minimum number of lowercase alphabetic characters that

must occur in the password. The default is zero, which means there is no

restriction of lowercase characters.

numeric The number of numeric digits that must occur in the password.

num Specifies the number of numeric digits that must occur in the password. The

numeric digits can range from 0 through 32 characters. The default is 0.

special-char The number of punctuation characters that must occur in the password.

char Specifies the number of punctuation characters that must occur in the

password. All printable, non-alphanumeric punctuation characters, except

colon (:) are allowed. The default value is 0.

Description Use this command to configure global password attributes.

Defaults The following are the default values of the global settings:

min-length—8 characters

max-retry—0

character-restriction (uppercase and lowercase)—0

• numeric-0

special-char—0

Command Modes Global configuration mode

Usage Guidelines Using the no form of the password-attributes command sets the default values of the individual

attributes.

```
Examples
           switch(config)# password-attributes ?
           Possible completions:
             character-restriction Set restriction on various types of character
             max-retry
                                Maximum number of login retires before which the user
           account is locked.
                                     Minimum length of the password.
             min-length
           switch(config)# password-attributes max-retry 4
           switch(config)# password-attributes character-restriction lower 2
           switch(config)# password-attributes character-restriction upper 1 numeric 1
           special-char 1
           switch(config)# exit
           switch# show running-config password-attributes
           password-attributes max-retry 4
           password-attributes character-restriction upper 1
           password-attributes character-restriction lower 2
           password-attributes character-restriction numeric 1
           password-attributes character-restriction special-char 1
           switch(config)# no password-attributes character-restriction lower
           switch(config)# no password-attributes character-restriction upper
           switch# show running-config password-attributes
           password-attributes max-retry 4
           password-attributes character-restriction numeric 1
           password-attributes character-restriction special-char 1
           switch# configure
           switch(config)# no password-attributes
           switch(config)# exit
           switch# show running-config password-attributes
           % No entries found.
```

See Also diag post, rule, service password-encryption, show running-config password-attributes

permit (extended ACLs)

Configures a MAC address rule to permit traffic based on the source and destination MAC addresses.

Synopsis permit [any | host MAC _ACL | MAC_ACL] [any | host MAC _ACL | MAC _ACL | [EtherType | arp |

fcoe | ipv4] [count]

 $\textbf{no permit [any | host } \textit{MAC _ACL} \mid \textit{MAC_ACL}] \; [\textbf{any | host } \textit{MAC _ACL} \mid \textit{MAC _ACL}] \; [\textit{EtherType | arp | left } \textit{MAC _ACL}] \; [\textbf{MAC _ACL}]$

fcoe | ipv4]

Operands any Specifies any source MAC address.

host *MAC_ACL* Specifies the source host MAC address for which to set permit conditions.

Use the format HHHH.HHHHH.

MAC ACL Specifies the destination host MAC address for which to set permit

conditions. Use the format HHHH.HHHHH.

any Specifies any destination MAC address.

host MAC_ACL Specifies the source host address for which to set permit conditions. Use the

format HHHH.HHHH.HHHH.

MAC_ACL Specifies the destination host address for which to set permit conditions.

Use the format HHHH.HHHH.

EtherType Specifies the protocol number for which to set the permit conditions. The

range of valid values is from 1536 through 65535.

arp Specifies to permit the Address Resolution Protocol (0x0806).

fcoe Specifies to permit the Fibre Channel over Ethernet Protocol (0x8906).

ipv4 Specifies to permit the IPv4 protocol (0x0800).

count Enables counting of the packets matching the filter rule.

Defaults By default, no MAC ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to configure rules to match and to permit traffic based on the source and

destination MAC addresses, and the protocol type. You can also enable counters for a specific rule. There are 255 ACL counters supported per port group. Use the **no permit** command to remove a

rule from the MAC ACL.

Usage Guidelines The first set of [any | host MAC_ACL | MAC_ACL] parameters is specific to the source MAC

address. The second set of [any | host MAC_ACL | MAC_ACL] parameters is specific to the

destination MAC address.

Examples To create a rule in a MAC extended ACL to permit IPv4 traffic from the source MAC address

0022.3333.4444 to the destination MAC address 0022.3333.5555 and to enable the counting of

packets:

switch(conf-macl-ext)#permit 0022.3333.4444 0022.3333.5555 ipv4 count

To delete a filter rule in a MAC extended ACL:

switch(conf-macl-ext)#no permit 0022.3333.4444 0022.3333.5555 ipv4

See Also mac access-list extended, mac access-list standard, seq (extended MAC ACLs), seq (standard MAC ACLs)

permit (standard ACLs)

Configures a MAC address rule to permit traffic based on the source MAC address.

Synopsis permit [MAC_ACL | any] [count]

no permit [MAC_ACL | any]

Operands MAC_ACL Specifies the source host MAC address for which to set permit conditions.

Use the format HHHH.HHHH.

any Specifies any source MAC address.

count Enables the counting of the packets matching the rule.

Defaults By default, no MAC ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to configure rules to match and to permit traffic based on the source MAC

address. You can also enable counters for a specific rule. There are 255 ACL counters supported

per port group. Use the no permit command to remove a rule from the MAC ACL.

Usage Guidelines There are no usage guidelines for this command.

Examples To create a rule in a MAC standard ACL to permit traffic from the source MAC address

0022.3333.4444 and to enable the counting of packets:

switch(conf-macl-std)#permit 0022.3333.4444 count

To delete a rule from a MAC standard ACL:

switch(conf-macl-std)#no permit 0022.3333.4444

See Also mac access-list extended, mac access-list standard, seq (extended MAC ACLs), seq (standard MAC

ACLs)

port-channel path-cost

Sets the path-cost behavior.

Synopsis port-channel path-cost [custom | standard]

Operands custom Specifies to use the custom behavior, which sets the path-cost changes

according to the port-channel's bandwidth.

standard Specifies to use the standard behavior, which sets that the path-cost does

not change according to port-channel's bandwidth.

Defaults The default path-cost is standard.

Command Modes Protocol Spanning Tree mode

Description Use this command to set the path-cost behavior for the port-channel.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the behavior for the path-cost to custom:

switch(conf-mstp)#port-channel path-cost custom

To set the behavior for the path-cost to standard:

switch(conf-mstp)#port-channel path-cost standard

2

port-profile

Creates a new AMPP port-profile in the fabric.

Synopsis port-profile profile-name [activate | qos-profile | security-profile | vlan-profile | static]

no port-profile profile-name

Operands profile-name A fabric-wide unique name of a port-profile.

activate Activates the specified profile

qos-profileEnters directly into edit mode for the QoS sub-profile.security-profileEnters directly into edit mode for the security sub-profile.vlan-profileEnters directly into edit mode for the VLAN sub-profile.

static Statically associates the profile VM MAC address.

Defaults There are no defaults for this command.

Command Modes Global configuration mode

Description This command creates a new AMPP port-profile in the fabric with the name specified, and enters

into the port-profile mode. If the port-profile name already exists, then the command enters the

port-profile mode and edits the existing profile.

A system-generated fabric-wide unique port-profile ID is assigned by default.

You can also directly access the sub-modes for the profile, and assign the profile statically to a

MAC address.

Use the no port-profile sample-profile activate version of the command to de-activate the

port-profile.

Examples None

port-profile-port

Activates AMPP port-profile configuration mode on a port.

Synopsis port-profile-port

no port-profile-port

Operands None

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description Use this command to activate AMPP port-profile configuration mode on the selected port.

selected port.

Examples switch(config)#interface tengigabitethernet 0/1

switch(conf-if-te-0/1)#port-profile-port

2

precedence

Sets the precedence of the CEE map.

Synopsis precedence value

Operands value The precedence value. The range of valid values is from 1 through 100.

Defaults The default value is 1.

Command Modes CEE map configuration mode

Description This command allows sets the precedence of the CEE map.

Usage Guidelines There are no usage guidelines for this command.

Examples switch(config-cee-map-default)#precedence 1

priority

Configures the priority for FCoE fabric-map mode.

Synopsis priority [priority]

no priority

Operands priority The priority value. The range of valid values is from 0 through 7.

Defaults The default priority value is 3.

Command Modes FCoE fabric-map configuration mode

Description This command configures the FCoE fabric-map priority.

Usage Guidelines The **no priority** command sets the value to the default value of 3.

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Examples switch(config)#fcoe

switch(config-fcoe)#fabric-map default
switch(config-fcoe-fabric-map)#priority 3

See Also fcoe

priority-group-table

Configures the bandwidth for each priority group.

Synopsis priority-group-table pgid [weight weight] [pfc on/off]

no priority-group-table pgid

Operands pgid Specifies the priority group ID (PGID) assigned to a priority group. The range

of valid values is from 15.0 through 15.7 for the eight reserved Strict Priority

PGIDs.

weight weight Maps a weight to a Deficit Weighted Round Robin (DWRR) scheduler queue.

This parameter is only valid for the DWRR Priority Group. The sum of all DWRR Priority Group weight values must equal 100 percent. The range of

valid values is from 1 through 100.

pfc Enables the Priority-based Flow Control (PFC) for each priority that gets

mapped to the priority group.

Defaults There is no default value for the weight. The PFC is disabled.

Command Modes CEE map configuration mode

Use this command to configure the bandwidth for each priority group, to associate a weight to a DWRR scheduler queue, and to enable the PFC.

You can define up to eight additional DWRR Priority Groups with the PGID values in the range of 0 to 7. Strict Priority Groups take priority in order from the lowest PGID value to the highest PGID value, for example, a PGID of 15.0 is a higher priority than a PGID of 15.1 and PGID of 15.1 is higher priority than PGID 15.2.

Use the **no priority-group-table** *pgid* command to return the priority group to the default values. For the Strict Priority Group, the PGID is still valid, but the PFC is disabled. For the DWRR Priority Group, the PGID is no longer valid and is deleted; the PGID can only be deleted when it is not bound to any Priority-to-Priority Group Table entry.

TABLE 1 Bandwidth allocation to user priority groups

PGID	PG%	PFC	Description
0	50	Υ	SAN
1	50	N	LAN

Usage Guidelines

A PGID value of 15 is a special value, which allows you to configure priorities with no bandwidth limit. The priority groups of 15.0 to 15.7 are pre-defined in the switch.

Examples

Description

To define the CEE map and configure the bandwidth with the priority group, use the values in Table 1.

```
switch(config)#cee-map test
switch(conf-ceemap)#priority-group-table 0 weight 50 pfc on
switch(conf-ceemap)#priority-group-table 1 weight 50
```

See Also

cee-map (FCoE), priority-table, show gos maps

priority-table

Provisions the CEE Priority-to-Priority Group Table.

Synopsis priority-table pgid0 pgid1 pgid2 pgid3 pgid4 pgid5 pgid6 pgid7

no priority-table

Operands pgidO Sets the Priority Group ID for all packets with CoS 0.

pgid1 Sets the Priority Group ID for all packets with CoS 1.
pgid2 Sets the Priority Group ID for all packets with CoS 2.
pgid3 Sets the Priority Group ID for all packets with CoS 3.
pgid4 Sets the Priority Group ID for all packets with CoS 4.
pgid5 Sets the Priority Group ID for all packets with CoS 5.
pgid6 Sets the Priority Group ID for all packets with CoS 6.

pgid7 Sets the Priority Group ID for all packets with CoS 7.

Defaults

The default CEE Priority mapping table matches the IEEE 802.1Q recommendation for systems supporting eight traffic classes. The 802.1Q maps CoS 0 (best effort) to Strict Priority Traffic Class 1 (PGID 15.6) and CoS 1 to below best effort Traffic Class 0 (PGID 15.7). All other CoS values go through unchanged, for example CoS 2 maps to Traffic Class 2 (PGID 15.5), up to CoS 7 and Traffic Class 7 (PGID 15.0).

Command Modes

CEE map configuration mode

Description

Use this command to provision the CEE Priority-to-Priority Group Table. This table maps each of the eight ingress CoS into a Priority Group. Use the **no priority-table** command to return the Priority mapping table to the default values.

Usage Guidelines

This table maps each of the eight ingress CoS into a Priority Group.

Only a single CoS can be mapped to a PFC-enabled priority queue. The CoS number must be identical to the priority queue number. If your configuration violates this restriction an error message displays and the Priority Group Table is set back to the default values.

When the CEE map is applied, and the interface is connected to the CNA, only one strict priority PGID (PGID 15.0 to PGID 15.7) is allowed.

TABLE 2 Mapping of incoming Priority-to-Priority Groups

Priority	PGID	
0	1	
1	1	
2	0	
3	1	
4	1	
5	1	

2

TABLE 2	Mapping of incoming Priority-to-Priority Groups (Continued)				
Priority	PGID				
6	1				
7	15.0				

Examples

To define a CEE map of the incoming Priority-to-Priority Groups, use the values in Table 2.

```
switch(config)#ceemap test
switch(conf-ceemap)#priority-table 1 1 0 1 1 1 1 15.0
```

See Also

cee, cee-map (Configuration), priority-group-table

profile

Creates an LLDP profile.

Synopsis profile name

no profile name

Operands name Assigns a name to the profile. The valid value is a maximum of 32

characters.

Defaults None

Command Modes Protocol LLDP configuration mode

Description Use this command to create an LLDP profile.

Usage Guidelines When you apply an LLDP profile on an interface using the Ildp profile command, it overrides the

global configuration. If a profile is not present, then the default global profile is used until you

create a valid profile. Up to 64 profiles can be created.

Examples To create a profile named test:

switch(conf-lldp)#profile test

To delete a profile named test:

switch(conf-lldp)#no profile test

See Also IIdp profile

2

protect-mode enable

Enables protect mode.

Synopsis protect-mode enable

no protect-mode enable

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description In the Blade Center Chassis environment, the Management Module (AMM) controls the operation

of the switch by configuring and initializing it. Protect mode of operation is a special mode which needs to be supported by both the switch and the AMM. Protect mode results in the AMM ceding control to the switch. The AMM loses its ability to perform some or all of the operations on the AMM. Once the AMM cedes control to the switch, the control can be given back to the AMM only by

disabling protect mode on the switch.

Once the switch enters protect mode, AMM's requests to perform any operations are ignored until the Network Administrator permits them. This behavior is preserved through power-cycles, even

after it is inserted into a different bay or chassis.

Usage Guidelines Use **no protect-mode enable** to disable this command.

Examples None

protocol IIdp

Enters the Link Layer Discovery Protocol (LLDP) configuration mode.

Synopsis protocol IIdp

no protocol IIdp

Operands None

Defaults The LLDP and DCBX protocols are enabled.

Command Modes Global configuration mode

Description Use this command to enter LLDP configuration mode to be able to make changes to the

parameters. Use the no protocol lldp command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To clear all LLDP configurations:

switch(config)#no protocol lldp

protocol spanning-tree

Synopsis protocol spanning-tree [mstp | rstp | stp | pvst | rapid-pvst]

no protocol spanning-tree

Operands mstp Specifies the Multiple Spanning Tree Protocol (MSTP).

rstp Specifies the Rapid Spanning Tree (RSTP).
stp Specifies the Spanning Tree Protocol (STP).

pvst Specifies Per-VLAN Spanning Tree Protocol (PVST).

rapid-pvst Specifies Rapid Per-VLAN Spanning Tree Protocol (RPVST).

Defaults By default, STP is not enabled. STP is not required in a loop-free topology.

Command Modes Global configuration mode

Description Use this command to create a context for the protocol specified. Use the **no protocol spanning-tree**

command to delete the context and all the configurations defined within the context or protocol for

the interface.

Usage Guidelines Consider enabling STP to detect or avoid loops. You must turn off one form of STP before turning

on another form.

Packet drops or packet flooding may occur if you do not enable xSTP on all devices connected on

both sides of parallel links.

Examples To enable the Spanning Tree Protocol:

switch(config)#protocol spanning-tree stp

See Also show spanning-tree

pwd

Print Working Directory displays the mode of the current working directory.

Synopsis pwd

Operands None

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to view the mode of the current working directory. This command functions in

global configuration mode and below.

Usage Guidelines There are no usage guidelines for this command.

Examples To view the current working directory:

switch2# pwd

syntax error: unknown argument.

switch# configure terminal

Entering configuration mode terminal

switch(config)# pwd

At top level switch(config)#

2

qos cos

Specifies the interface Class of Service (CoS) value.

Synopsis qos cos value

no gos cos

Operands value Specifies the CoS value. The range of valid values is from 0 through 7.

Defaults The default CoS value is 0 (zero).

Command Modes Interface configuration mode

Description Use this command to specify the interface Default CoS value. When Interface ingress QoS Trust is

in the untrusted mode, then the Interface Default CoS value is applied to all ingress traffic for user priority mapping. When the interface ingress QoS Trust is in the CoS mode, then the Interface Default CoS value is applied to all non-priority tagged ingress traffic for user priority mapping. Use

the no gos cos command to return the CoS value to the default.

Usage Guidelines If the interface is QoS trusted, the CoS value of the interface is used to assign a CoS value to all

untagged packets entering the interface.

This command is unavailable in VCS mode. QoS Trust is implicitly turned on when the QoS CoS-Mutation map is applied to interfaces, and is implicitly turned off when the QoS CoS-Mutation

map is removed.

Examples To set the interface CoS value to 2:

switch(conf-if-te-0/2)#qos cos 2

To return the interface CoS value to the default:

switch(conf-if-te-0/2)#no qos cos

See Also show gos interface, gos map cos-traffic-class, gos trust cos

qos cos-mutation

Applies a CoS-to-CoS mutation QoS map on an interface.

Synopsis qos cos-mutation name

no gos cos-mutation

Operands name Specifies the name of the CoS mutation map.

Defaults There is no explicit CoS-to-CoS mutation QoS map applied; by default the inbound CoS equals the

outbound CoS.

Command Modes Interface configuration mode

Description Use this command to apply a CoS-to-CoS mutation QoS map on an interface.

Usage Guidelines This command applies a CoS-to-CoS mutation map on an interface. The qos cos-mutation

command is not available if the interface is in CEE Provisioning mode. Use the **no qos**

cos-mutation command to remove the CoS-to-CoS mutation map.

Examples To activate the CoS-to-CoS mutation QoS map on the interface:

switch(conf-if-te-0/1)#qos cos-mutation test

To remove the CoS-to-CoS mutation QoS map on the interface:

switch(conf-if-te-0/1)#no qos cos-mutation

See Also qos map cos-mutation, show qos maps

qos cos-traffic-class

Applies a CoS-to-Traffic Class QoS map on an interface.

Synopsis qos cos-traffic-class name

no qos cos-traffic-class

Operands name Specifies the name of a previously created CoS-to-Traffic Class QoS map.

Only one CoS-to-Traffic Class QoS map can exist at a time. An existing CoS-to-Traffic Class QoS map must be removed before a new one can be

applied.

Defaults There is no explicit CoS-to-Traffic Class QoS map applied; the implicit behavior is to match the IEEE

802.1Q recommendations for systems supporting eight Traffic Classes.

Command Modes Interface configuration mode

Description Use this command to apply a CoS-to-Traffic Class QoS map to an interface. Use the **no qos**

cos-traffic-class command to remove the CoS-to-Traffic Class mapping.

Usage Guidelines This command is not available when the interface is in the CEE Provisioning mode.

Examples To apply a CoS-to-Traffic Class QoS map to an interface:

switch(conf-if-te-0/1)#qos cos-traffic-class test

See Also qos map cos-traffic-class, qos trust cos, qos cos-mutation, show qos maps

qos flowcontrol

Activates and configures QoS flow control.

Synopsis qos flowcontrol tx [on | off] rx [on | off]

no qos flowcontrol

Operands tx [on | off] Activates or deactivates the transmission portion of flow control.

rx [on | off] Activates the receiving portion of flow control.

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description This command configures and activates QoS flow control.

Usage Guidelines In VCS mode, this command does not take effect and will result in a error. Legacy flow control

cannot be enabled if the switch is in VCS mode.

Examples None

qos flowcontrol pfc cos

Activates and configures flow control for CoS.

Synopsis qos flowcontrol pfc cos tx [on | off] rx [on | off]

no qos flowcontrol pfc cos

Operands tx [on | off] Activates or deactivates the transmission portion of flow control.

rx [**on** | **off**] Activates the receiving portion of flow control.

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description In VCS mode, this command only affects per-interface pause behavior. To use flow control in VCS

mode, use the CEE map configuration.

Usage Guidelines In VCS mode, this command only takes effect on the interface. In order to have PFC functionality

through the VCS cluster, use the CEE map configuration.

Examples None

qos map cos-mutation

Creates a QoS map for performing CoS-to-CoS mutation.

Synopsis qos map cos-mutation name cos0 cos1 cos2 cos3 cos4 cos5 cos6 cos7

no gos map cos-mutation name

Operands	name	Specifies a unique name across all CoS-to-CoS mutation QoS maps defined within the system. If the named CoS-to-CoS mutation QoS map does not exist, then it is created. If the named CoS-to-CoS mutation QoS map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the QoS map.
	cos0	Sets the outbound CoS value for all packets with inbound CoS 0.
	cos1	Sets the outbound CoS value for all packets with inbound CoS 1.
	cos2	Sets the outbound CoS value for all packets with inbound CoS 2
	cos3	Sets the outbound CoS value for all packets with inbound CoS 3.
	cos4	Sets the outbound CoS value for all packets with inbound CoS 4.
	cos5	Sets the outbound CoS value for all packets with inbound CoS 5.
	cos6	Sets the outbound CoS value for all packets with inbound CoS 6.
	cos7	Sets the outbound CoS value for all packets with inbound CoS 7.

Defaults There are no CoS-to-CoS mutation QoS maps defined.

Command Modes Global configuration mode

Description

Use this command to create a QoS map for performing CoS-to-CoS Mutation. A CoS-to-CoS mutation takes an inbound CoS value and maps it to an outbound CoS value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied. The outbound CoS value is used in selecting Traffic Class and egress packet marking. The default is no CoS-to-CoS Mutation QoS maps defined.

Usage Guidelines

Use the **no qos map cos-mutation** *name* command to delete the named CoS-to-CoS mutation QoS map. A OoS map can only be deleted if it is not bound to any interface.

Examples

To create a CoS-to-CoS mutation QoS map to swap CoS 4 and CoS 5 and apply it on an interface, for example inbound CoS 4 is mapped to outbound CoS 5 and inbound CoS 5 is mapped to outbound CoS 4; all other CoS values go through unchanged:

```
switch(config)#qos map cos-mutation test 0 1 2 3 5 4 6 7
switch(config)#interface tengigabitethernet 0/1
switch(conf-if-te-0/1)#qos cos-mutation test
```

To delete a CoS-to-CoS mutation QoS map:

switch(config)#no qos map cos-mutation test

See Also gos cos-mutation, show gos maps

qos map cos-traffic-class

Creates a QoS map for performing CoS-to-Traffic Class mapping.

Synopsis qos map cos-traffic-class name tc0 tc1 tc2 tc3 tc4 tc5 tc6 tc7

no qos map cos-traffic-class

Operands.	name	Specifies the CoS-to-Traffic Class QoS map name. If the named CoS-to-Traf Class QoS map does not exist, then it is created. If the named CoS-to-Traf Class QoS map already exists, then it is updated and new mappings are automatically propagated to all interfaces bound to the QoS map.		
	tc0	Sets the Traffic Class value for all packets with outbound CoS 0.		
	tc1	Sets the Traffic Class value for all packets with outbound CoS 1.		
	tc2	Sets the Traffic Class value for all packets with outbound CoS 2.		
	tc3	Sets the Traffic Class value for all packets with outbound CoS 3.		
	tc4	Sets the Traffic Class value for all packets with outbound CoS 4.		
	tc5	Sets the Traffic Class value for all packets with outbound CoS 5.		
	tc6	Sets the Traffic Class value for all packets with outbound CoS 6.		
	tc7	Sets the Traffic Class value for all packets with outbound CoS 7.		

Defaults There are no CoS-to-Traffic Class QoS maps defined.

Command Modes Global configuration mode

Description

Use this command to create a QoS map for performing CoS-to-Traffic Class mapping. A CoS-to-Traffic Class QoS map takes an outbound CoS value and maps it to a Traffic Class. The outbound CoS value is used as the packet user priority after applying the configured interface QoS trust, interface default CoS, and CoS-to-CoS mutation policies. Traffic Class is a reference to a scheduler queue and packet servicing policy. Use the **no qos map cos-traffic-class** name command to delete the CoS-to-Traffic Class QoS map specified by the name. The CoS-to-Traffic Class QoS map can only be deleted when it is not bound to any interface. All other CoS values go through unchanged. This mapping matches the default behavior recommended in IEEE 802.1Q for systems supporting eight Traffic Classes.

Usage Guidelines

There are no usage guidelines for this command.

Examples

To create a CoS-to-Traffic Class QoS map to map CoS 0 to Traffic Class 1 and CoS 1 to Traffic Class 0:

switch(config)#qos map cos-traffic-class test 1 0 2 3 4 5 6 7

To delete a CoS-to-Traffic Class QoS map:

switch(config)#no qos map cos-traffic-class test

See Also

gos map cos-mutation, gos trust cos

qos-profile (AMPP)

Activates the QoS profile mode for AMPP.

Synopsis qos-profile

Operands None

Defaults There are no defaults for this command.

Command Modes Port-profile mode

Description This command activates the QoS profile mode for AMPP. This mode allows configuration of QoS

attributes of a port-profile.

Usage Guidelines There are no usage guidelines for this command.

Examples Switch(config)#port-profile sample-profile

Switch(conf-pp)#qos-profile

qos queue multicast scheduler

Configures the multicast Traffic Class packet expansion scheduler policy. All multicast Traffic Class packet expansion queues are serviced Deficit Weighted Round Robin (DWRR).

Synopsis

qos queue multicast scheduler dwrr mTC0_WEIGHT mTC1_WEIGHT mTC2_WEIGHT mTC3_WEIGHT mTC4_WEIGHT mTC5_WEIGHT mTC6_WEIGHT mTC7_WEIGHT

no dos queue multicast scheduler

	no qos queue multicast scheduler				
Operands dwrr		Configures the DWRR multicast Traffic Class packet expansion policy.			
	mTCO_WEIGHT	Sets the DWRR weight for multicast Traffic Class 0 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.			
	mTC1_WEIGHT	Sets the DWRR weight for multicast Traffic Class 1 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.			
	mTC2_WEIGHT	Sets the DWRR weight for multicast Traffic Class 2 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.			
	mTC3_WEIGHT	Sets the DWRR weight for multicast Traffic Class 3 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.			
	mTC4_WEIGHT	Sets the DWRR weight for multicast Traffic Class 4 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.			
	mTC5_WEIGHT	Sets the DWRR weight for multicast Traffic Class 5 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.			
	mTC6_WEIGHT	Sets the DWRR weight for multicast Traffic Class 6 packet expansion in units of handwidth percentage. The sum of all weight values must equal 100			

of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.

mTC7_WEIGHT Sets the DWRR weight for multicast Traffic Class 7 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. The range of valid values is from 0 through 100.

Defaults The default weight value is 25 percent bandwidth for each multicast Traffic Class.

Command Modes Global configuration mode

Description

Use this command to configure the multicast Traffic Class packet expansion scheduler policy. All multicast Traffic Class packet expansion queues are serviced Deficit Weighted Round Robin (DWRR). This multicast Traffic Class packet expansion scheduler policy is applied uniformly across the entire system. Use the no gos queue multicast scheduler command to return the multicast Traffic Class packet expansion scheduler to the default value.

Usage Guidelines There are no usage guidelines for this command.

Examples

To set the multicast Traffic Class packet expansion scheduler for Traffic Class 0 getting 10 percent bandwidth, Traffic Class 1 getting 20 percent bandwidth, Traffic Class 2 getting 30 percent bandwidth, and Traffic Class 3 getting 40 percent bandwidth:

switch(config)#qos queue multicast scheduler dwrr 10 20 30 40

To return the system to the default multicast Traffic Class packet expansion scheduler policy:

switch(config)#no qos queue multicast scheduler

See Also

qos rcv-queue multicast rate-limit

qos queue scheduler

Configures the Traffic Class packet scheduler policy.

Synopsis

qos queue scheduler strict-priority strict-priority-number dwrr weight0 weight1 weight2 weight3

weight4 weight5 weight6 weight7

no qos queue scheduler

Operands strict-priority

Configures the Strict Priority Traffic Class policy. All Strict Priority Traffic

Classes are serviced before any DWRR Traffic Classes.

strict-priority-number

Sets the number of the Strict Priority Traffic Class. This is the strict priority number of the highest Traffic Class. For example, if the strict priority number is 3, the strict priority Traffic Class contains Traffic Classes 7, 6, and 5. The

range of valid values is from 0 through 8.

dwrr Configures the DWRR Traffic Class policy. There are a variable number of

DWRR weight values accepted that are dependent on the setting of strict priority number. The strict priority number plus the number of DWRR weight

values must always add up to 8 Traffic Classes.

weight0 Sets the DWRR weight for Traffic Class 0 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The weight0 value is only valid when the strict priority number is less than 8. The range of valid values is from 0

through 100 percent.

weight1 Sets the DWRR weight for Traffic Class 1 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight1* value is only valid when the strict priority number is less than 7. The range of valid values is from 0

through 100 percent.

weight2 Sets the DWRR weight for Traffic Class 2 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The weight2 value is only valid when the strict priority number is less than 6. The range of valid values is from 0

through 100 percent.

weight3 Sets the DWRR weight for Traffic Class 3 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The weight3 value is only valid when the strict priority number is less than 5. The range of valid values is from 0

through 100 percent.

weight4 Sets the DWRR weight for Traffic Class 4 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The weight4 value is only valid when the strict priority number is less than 4. The range of valid values is from 0

through 100 percent.

weight5 Sets the DWRR weight for Traffic Class 6 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight5* value is only valid when the strict priority number is less than 3. The range of valid values is from 0

through 100 percent.

weight6 Sets the DWRR weight for Traffic Class 6 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The weight6 value is only valid when the strict priority number is less than 2. The range of valid values is from 0

through 100 percent.

weight 7 Sets the DWRR weight for Traffic Class 7 in units of bandwidth percentage

left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The weight7 value is only valid when the strict priority number is less than 1. The range of valid values is from 0

through 100 percent.

Defaults The default strict priority value is 8. There is no default value for each weight value.

Command Modes Global configuration mode

Description Use this command to configure the Traffic Class packet scheduler policy. Eight Traffic Classes are

supported with a configurable number of them being Strict Priority and any remaining ones being serviced DWRR. This Traffic Class packet scheduler policy is applied uniformly across the entire system. Actual Traffic Class packet scheduling is performed independently by each switch.

Usage Guidelines In VCS mode, this command does not take effect and will result in a error. To update the

scheduling, please use the CEE map configuration.

Use the **no qos queue scheduler** command to return the Traffic Class packet scheduler to the

default value.

Examples To set the Traffic Class packet scheduler for 4 Strict Priority Traffic Class and 4 DWRR Traffic Class with Traffic Class 0 getting 10 percent bandwidth, Traffic Class 1 getting 20 percent bandwidth,

Traffic Class 2 getting 30 percent bandwidth, and Traffic Class 3 getting 40 percent bandwidth:

switch(config)#qos queue scheduler strict-priority 4 dwrr 10 20 30 40

To return the system to the default Traffic Class packet scheduler policy:

switch(config)#no qos queue scheduler

See Also qos rcv-queue multicast rate-limit, qos rcv-queue multicast threshold

qos rcv-queue multicast rate-limit

Configures a cap on the maximum rate for multicast packet expansion.

Synopsis qos rcv-queue multicast rate-limit rate [burst burst-size]

no qos rcv-queue multicast rate-limit

Operands rate Specifies the maximum rate for multicast packet expansion in units of

packets per second (pkt/s). The range of valid values is from 6500 through

20000000 pkt/s.

burst burst-size Configures a cap on the maximum burst size for multicast packet expansion,

for example packet replication. The range of valid values is from 50 through

65535 packets.

Defaults The default burst size is 4096 packets. The default rate value is 3000000 pkt/s.

Command Modes Global configuration mode

Description Use this command to configures a cap on the maximum rate for multicast packet expansion, for

example packet replication. This rate limit is applied uniformly across the entire system. This rate limit is enforced independently by each switch. Use the **no qos rcv-queue multicast rate-limit**

command to return the multicast packet expansion rate limit to the default settings.

The *rate* operand places a cap on the sum of the first level expansion, for example the ingress packets replicated for each egress switch plus the second level expansion, for example packets

replicated for egress interfaces on the switch.

The burst burst-size operand represents the maximum number of multicast packet expansion that

can be performed back-to-back as a single burst in units of packets (pkt).

Usage Guidelines There are no usage guidelines for this command.

Examples To lower the maximum multicast packet expansion rate to 10000 pkt/s:

switch(config)#qos rcv-queue multicast rate-limit 10000

To return the system to the default multicast packet expansion rate limit values:

switch(config)#no qos rcv-queue multicast rate-limit

See Also qos rcv-queue multicast threshold

qos rcv-queue multicast threshold

O				-l + l - 4 -			
Configures a car	on the	· maxımum	aueue	depth to	r muiticast	раскет ех	bansion dueues.

Synopsis qos rcv-queue multicast threshold mTC0 mTC1 mTC2 mTC3 mTC4 mTC5 mTC6 mTC7

no gos rcv-queue multicast threshold

Operands	mTC0	Sets the Tail Drop Threshold for multicast Traffic C	lass 0 packet expansion
----------	------	--	-------------------------

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC1 Sets the Tail Drop Threshold for multicast Traffic Class 1 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC2 Sets the Tail Drop Threshold for multicast Traffic Class 2 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC3 Sets the Tail Drop Threshold for multicast Traffic Class 3 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC4 Sets the Tail Drop Threshold for multicast Traffic Class 4 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC5 Sets the Tail Drop Threshold for multicast Traffic Class 5 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC6 Sets the Tail Drop Threshold for multicast Traffic Class 6 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

mTC7 Sets the Tail Drop Threshold for multicast Traffic Class 7 packet expansion

queue in units of packets (pkt). The range of valid values is from 0 through

16383 packets.

Command Modes Global configuration mode

Description Use this command to configure a cap on the maximum queue depth for multicast packet

expansion queues. The individual Tail Drop Threshold is specified for each of the four multicast traffic classes. These Tail Drop Thresholds are applied uniformly across the entire system. These queue depths are enforced independently by each switch. Use the **no qos rcv-queue multicast**

threshold command to return the multicast expansion guegues to the default value.

Usage Guidelines There are no usage guidelines for this command.

Examples To increase multicast packet expansion Tail Drop Threshold to 1000 pkt for each multicast Traffic

Class:

To return the system to the default multicast packet expansion Tail Drop Threshold value:

switch(config)#no qos rcv-queue multicast threshold

See Also qos rcv-queue multicast rate-limit

qos trust cos

Specifies the interface QoS trust mode for incoming traffic.

Synopsis qos trust cos

no qos trust cos

Operands None

Defaults The QoS trust mode set to the untrusted state.

Command Modes Interface configuration mode

Description Use this command to specify the interface ingress QoS trust mode, which controls user priority

mapping of incoming traffic. The untrusted mode overrides all incoming priority markings with the Interface Default CoS. The CoS mode sets the user priority based on the incoming CoS value, if the incoming packet is not priority tagged, then fallback is to the Interface Default CoS value. Use the

no gos trust cos command to return to the default.

Usage Guidelines When a CEE map is applied on an interface, the qos trust cos command is not allowed. The CEE

map always puts the interface in the CoS trust mode. This command is not applicable for

port-channel interfaces.

Examples To set the interface QoS to the trust mode:

```
switch(conf-if-te-0/1)#qos trust cos
```

To return the interface QoS to the default value or to the untrusted state:

```
switch(conf-if-te-0/1)#no qos trust cos
```

When a CEE map is applied, the switch does not allow the **qos trust cos** command and displays the following error:

```
switch(conf-if-te-0/1)#cee demo
switch(conf-if-te-0/1)#qos trust cos
% Error: QoS is not in non-CEE Provisioning mode
```

See Also qos cos, show qos maps

radius-server

Applies attributes to the RADIUS server.

Synopsis radius-server host <nostname> | <ip-address> [auth-port port] [timeout sec]

[retransmit num] [key shared-secret-string] [protocol chap | pap | ms-chap-peap]

no radius-server host hostname | ip-address

Operands host Identifies the RADIUS server by host name or IP address.

hostname Specifies the host name of the RADIUS server.

ip-address Specifies the IP address of the RADIUS server. IPv4 and IPv6 are supported.

auth-port The authentication port.

port Specifies the UDP port used to connect the RADIUS server for

authentication. The default is 1812.

timeout The time to wait for the RADIUS server to respond.

sec Specifies the timeout value, in seconds. The default is 5 seconds.

retransmit The number of times the switch tries to connect to a RADIUS server.

num Specifies the number of tries to connect to a RADIUS server. The default is 5

attempts.

key The shared secret between the switch and the RADIUS server.

shared-secret-string

The text string that is used as the shared secret between the switch and the

RADIUS server. The default is sharedsecret.

protocol The authentication protocol to be used.

chap | pap | ms-chap-peap

Specifies the authentication protocol. Options include CHAP, PAP,

Use this command to configure attributes on the RADIUS server. If the RADIUS server doesn't exist,

PEAP-MSCHAP. The default is CHAP.

it is duded. If the tyrbles server arready exists, then the dittributes are

it is added. If the RADIUS server already exists, then the attributes are changed.

Defaults The following are the default values of the global settings

host—There is no default for the host:

• auth-port—UDP port 1812

timeout—5 seconds

• retransmit—5 attempts

key—sharedsecret

protocol—CHAP

Command Modes Global configuration mode

Description

Usage Guidelines

Using the **no** form of the radius-server command sets the default values of the individual attributes.

Examples Examples

Example of adding a RADIUS server:

```
switch(config) # radius-server ?
Possible completions:
  <hostname: IP Address of this RADIUS server>
switch(config)# radius-server host
switch(config)# radius-server host 10.24.65.6 ?
Possible completions:
             UDP Port for Authentication (default=1812)
  auth-port
             Authentication protocol to be used (default=CHAP)
 protocol
              Secret shared with this server (default='sharedsecret')
 kev
 retransmit Number of retries for this server connection (default=5)
  timeout
              Wait time for this server to respond (default=5 sec)
switch(config) # radius-server host 10.24.65.6
switch(config)# radius-server host 10.24.65.6 protocol chap ?
Possible completions:
  auth-port UDP Port for Authentication (default=1812)
              Secret shared with this server (default='sharedsecret')
 retransmit Number of retries for this server connection (default=5)
              Wait time for this server to respond (default=5 sec)
switch(config)# radius-server host 10.24.65.6 protocol chap retransmit ?
Possible completions:
  <0-100> [5]
switch(config)# radius-server host 10.24.65.6 protocol chap retransmit 100
switch(config-radius-server-10.24.65.6)#
switch(config)# radius-server host 10.38.37.180 protocol pap key
"new#virgo*secret timeout 10
```

Example of changing a RADIUS server:

```
switch(config)# radius-server host ?
Possible completions:
    <hostname: IP Address of this RADIUS server> 10.38.37.180 10.24.65.6
switch(config)# radius-server host 10.38.37.180
switch(config-host-10.38.37.180)# key ?
Possible completions:
    <string>[new#virgo*secret]
switch(config-host-10.37.37.180)# key "changedsec"
switch(config-host-10.37.37.180)# no timeout
```

See Also

show running-config radius-server, show running-config tacacs-server, tacacs-server

2

region

Specifies the Multiple Spanning Tree Protocol (MSTP) region.

Synopsis region region-name

no region

Operands region-name Assigns a name to an MSTP region.

Defaults There are no default configurations for this command.

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to assign a name to an MSTP region. Use the **no region** command to delete the

name.

Usage Guidelines The *region-name* string has a maximum length of 32 characters and is case-sensitive.

Examples To assign a name to an MSTP region named brocade1:

switch(config)#protocol spanning-tree mstp

switch(conf-mstp)#region brocade1

See Also revision, show spanning-tree

reload

Reboots the control processor (CP).

Synopsis reload

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to perform a "cold reboot" (power off and restart) of the control processor.

Usage Guidelines The reload operation is disruptive, and the command prompts for confirmation before executing.

When you reboot a switch connected to a fabric, all traffic to and from that switch stops. All ports

on that switch remain inactive until the switch comes back online.

Examples To perform a cold reboot on the switch:

switch(config)#reload

Are you sure you want to reload the switch [y/n]?: y

See Also fastboot

2

remap fabric-priority

Remaps the CoS fabric priority.

Synopsis remap fabric-priority priority

Operands priority Specifies the remapped CoS priority value for VCS. The range of valid values

is from 0 through 7.

Defaults The default value is 0.

Command Modes CEE map configuration mode

Description This command remaps the CoS fabric priority to a different priority for VCS.

Usage Guidelines There are no usage guidelines for this command.

Examples None

remap lossless-priority

Remaps the VCS fabric priority.

Synopsis remap lossless-priority priority

Operands priority Specifies the remapped priority value. The range of valid values is from 0

through 7.

Defaults The default value is 0.

Command Modes CEE map configuration mode

Description This command remaps the VCS lossless priorities to a different priority.

Usage Guidelines There are no usage guidelines for this command.

Examples None

rename

Renames a file in the switch flash memory.

Synopsis rename current_name new_name

Operands *current_name* Specifies the file name you wish to change.

new_name Specifies the new file name.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to rename a user-generated file in the switch flash memory.

Usage Guidelines This command is supported only on the local switch.

System files cannot be renamed. If you try to rename a system file, an appropriate message is

displayed.

Examples To rename a file:

```
switch# rename myconfig.vcs myconfig.old
switch# dir
total 24
                                4096 Feb 13 00:39 .
drwxr-xr-x 2 root
                    sys
                                4096 Jan 1 1970 ...
drwxr-xr-x 3 root root
-rwxr-xr-x 1 root sys
                                417 Oct 12 2010 myconfig.old
-rwxr-xr-x 1 root
                                417 Oct 12 2010 defaultconfig.novcs
                    sys
                                697 Oct 12 2010 defaultconfig.vcs
-rwxr-xr-x 1 root
                    sys
                                6800 Feb 13 00:37 startup-config
-rw-r--r-- 1 root
                    root
```

See Also

copy, copy running-config startup-config, delete, dir, show file, show running-config, show support, vcs

resequence access-list mac

Specifies the renumbering of the rules in a MAC ACL.

Synopsis resequence access-list mac [name | seq_num | increment]

Operands name Specifies the name of a standard or an extended MAC ACL.

seq_num Specifies the starting sequence number in the MAC ACL. The range of valid

values is from 1 through 65535.

increment Specifies a value to increment the sequence number between rules. The

range of valid values is from 1 through 65535.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to reassign sequence numbers to entries of an existing MAC access-list.

Usage Guidelines Reordering the sequence numbers is useful when you need to insert rules into an existing MAC

ACL and there are not enough sequence numbers available. When all sequence numbers between rules are exhausted, this feature allows the reassigning of new sequence numbers to entries of an

existing access list.

Examples To reorder the rules in a MAC ACL:

```
switch#show running-config access-list mac test
!
mac access-list standard test
seq 1 permit 0011.2222.3333
seq 2 permit 0011.2222.4444
seq 3 permit 0011.2222.5555
seq 4 deny 0011.2222.6666
!
```

switch#resequence access-list mac test 10 10

```
switch#show running-config access-list mac test
!
mac access-list standard test
seq 10 permit 0011.2222.3333
seq 20 permit 0011.2222.4444
seq 30 permit 0011.2222.5555
seq 40 deny 0011.2222.6666
!
```

See Also mac access-list extended, seq (standard MAC ACLs)

2

revision

Assigns a version number to the Multiple Spanning Tree Protocol (MSTP) configuration.

Synopsis revision number

no revision

Operands *number* Specifies the revision or version number of the MSTP region. The range of

valid values is from 0 through 255.

Defaults The default is 0.

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to specify the configuration revision number. Use the **no revision** command to

return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the configuration revision to 1:

switch(config)#protocol spanning-tree mstp

switch(conf-mstp)#revision 1

See Also region, show spanning-tree

rmon alarm

Sets the RMON alarm conditions.

Synopsis rmon alarm index snmp_oid interval seconds [absolute | delta] rising-threshold value event

number [falling-threshold value event number [owner name] | owner name]

no rmon alarm

Operands index Specifies the RMON alarm index. The range of valid values is from 1 through

65535.

snmp_oid Specifies the MIB object to monitor. The variable must be in the SNMP OID

format, for example, 1.3.6.1.2.1.16.1.1.1.5.65535. The object type must be

a counter32.

interval seconds Specifies the RMON alarm sample interval in seconds. The range of valid

values is from 1 through 2147483648.

absolute Sets the sample type as absolute.

delta Sets the sample type as delta.

rising-threshold value

Specifies the RMON alarm rising threshold. The range of valid values is from

0 through 4294967295.

event number Specifies the event for the rising alarm. The range of valid values is from 1

through 65535.

falling-threshold value

Specifies the RMON alarm falling threshold. The range of valid values is from

0 through 4294967295.

event number Specifies the event for the rising alarm. The range of valid values is from 1

through 65535.

owner name Specifies the identity of the owner. The maximum number of characters is

32.

Defaults There are no alarms configured.

Command Modes Global configuration mode

Description Use this command to set alarm conditions. Use the **no rmon alarm** command to disable the alarm

conditions.

Usage Guidelines There are no usage guidelines for this command.

Examples To set RMON alarm conditions:

switch(config)#rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.65535 interval 5
absolute rising-threshold 10000 event 100 falling-threshold 1000 event 101

owner admin

See Also rmon event, show rmon

rmon collection history

Collects the periodic statistical samples of Ethernet group statistics on an interface for later

retrieval.

Synopsis rmon collection history number [buckets bucket_number | interval seconds | owner name]

no romn collection history

Operands number Specifies the RMON collection control index value. The range of valid values

is from 1 through 65535.

buckets bucket_number

Specifies the maximum number of buckets for the RMON collection history.

The range of valid values is from 1 through 65535.

interval seconds Specifies the alarm sample interval in seconds. The range of valid values is

from 1 through 2147483648.

owner name Specifies the identity of the owner. The maximum number of characters is

32.

Defaults The collection of RMON history is not enabled.

Command Modes Interface configuration mode

Description Use this command to collect Ethernet group statistics on an interface. Use the **no rmon collection**

history command to disable the history.

Usage Guidelines There are no usage guidelines for this command.

Examples To collect RMON statistics for the owner admin on 10 Gbps Ethernet interface 0/1:

switch(config)#interface tengigabitethernet 0/1
switch(conf-if-te-0/1)#rmon collection history 5

See Also show rmon history

rmon collection stats

Collects Ethernet group statistics on an interface.

Synopsis rmon collection stats *number* [owner *name*]

no rmon collection stats

Operands number Specifies the RMON collection control index value. The range of valid values

is from 1 through 65535.

owner name Specifies the identity of the owner.

Defaults The collection of RMON statistics is not enabled.

Command Modes Interface configuration mode

Description Use this command to collect Ethernet group statistics on an interface. Use the **no rmon collection**

stats command to disable the collection of statistics.

Usage Guidelines There are no usage guidelines for this command.

Examples To collect RMON statistics for the owner admin on 10 Gbps Ethernet interface 0/1:

switch(config)#interface tengigabitethernet 0/1

switch(conf-if-te-0/1)#rmon collection stats 2 owner admin

See Also show rmon history

rmon event

Adds or removes an event in the RMON event table associated to the RMON alarm number.

Synopsis rmon event index [description word] [log] [owner name] [trap word]

no rmon event

Operands index Specifies the RMON event number. The range of valid values is from 1

through 65535.

description word Specifies a description of the event.

log Generates an RMON log when an event is triggered.

owner name Specifies the owner of the event. The maximum number of characters is 32.

trap word Specifies the SNMP community or string name to identify this trap.

Defaults There are no events configured.

Command Modes Global configuration mode

Description Use this command to add or remove an event in the RMON event table that is associated with an

RMON alarm number. Use the no rmon event command to remove the event configuration.

Usage Guidelines There are no usage guidelines for this command.

Examples To configure an RMON event:

switch(config) #rmon event 2 log description "My Errorstoday" owner gjack

See Also show rmon history

2

role name

The role name command allows you to create roles dynamically and later associate them with

rules to define the permissions applicable to a particular role.

Synopsis role name role name [desc description]

no role name

Operands role_name The name of the role.

desc A description of the role.

description Provides a description to identify the role.

Description Use this command to create a new role.

Defaults There are no defaults for this command.

Command Modes Global configuration mode

Usage Guidelines The maximum number of roles is 64. Using the no form of the role command sets the default

values of the individual attributes.

Examples The following example describes how to assign a role to a user and then create a role for the user.

switch(config)# username NetworkSecurityAdmin role NetworkSecurityAdmin password

testpassword

switch(config)# role name NetworkSecurityAdmin desc "Manages VCS switches"

See Also rule, show running-config role, show running-config rule

2

rule

rule

A rule defines the permissions applicable to a particular role.

Synopsis rule index action [accept | reject] operation [read-only | read-write] role name

command command_name

no rule index>

Operands index Specifies the numeric identifier of the rule. The valid range is from

1 through 8000.

action Indicates whether the user associated with this role can or cannot

execute the command.

to execute the command.

operation Indicates if the rule is read-only or read-write.

read-only | read-write Specifies the type of operation. Read-write is the default.

role The name of the role for which the rule is defined.

name Specifies the name of the role for which the rule is defined.

command The command on which access must be defined. This is the command that

gets executed. Separate commands with options with spaces. There are four supported commands with options: **copy**, **clear**, **interface**, and **protocol**.

command nameSpecifies the name of the command on which access must be defined.

Description Use this command to create a rule that can be associated with a role.

Defaults The following are the default values of the global settings:

action—accept

operation—read-write

Command Modes Global configuration mode

Usage Guidelines When adding a rule, the role and command operands are mandatory and the action and operation

operands are optional. The maximum number of rules is 512.

When changing a rule, all operands except index are optional.

Examples Example of adding a rule:

switch(config)# rule 150 action accept operation read-write role NetworkAdmin

command config

See Also diag post, show running-config role, show running-config rule

run-script

Used to run a script file on the switch.

Synopsis run-script [flash://]filename]

Operands filename Name of the script file in the flash memory.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to run a script file residing in the flash memory.

Usage Guidelines The scripting support only supports textual configuration files. It does not handle any scripting

languages, such as Tcl, Expect, and so on.

Examples None

security-profile (AMPP)

Activates the security-profile mode for AMPP.

Synopsis security-profile

Operands None

Defaults There are no defaults for this command.

Command Modes Port-profile mode

Description This command activates the security-profile mode for AMPP. This mode allows configuration of

security attributes of a port-profile.

Usage Guidelines There are no usage guidelines for this command.

Examples Switch(config)#port-profile sample-profile

Switch(conf-pp)#security-profile

seq (extended MAC ACLs)

Inserts a rule anywhere in the MAC ACL.

Synopsis seq value [deny | permit] [any | host MAC _ACL | MAC_ACL] [any | host MAC _ACL | MAC _ACL]

[EtherType | arp | fcoe | ipv4] [count]

no seq value

Operands value Specifies the sequence number for the rule. The range of valid values is from

0 through 65535.

permit Specifies rules to permit traffic.

deny Specifies rules to deny traffic.

any Specifies any source MAC address.

host MAC_ACL Specifies the source host MAC address for which to set permit or deny

conditions. Use the format HHHH.HHHHH.

MAC_ACL Specifies the destination host MAC address for which to set permit or deny

conditions. Use the format HHHH.HHHHH.

any Specifies any destination MAC address.

host *MAC_ACL* Specifies the source host address for which to set permit or deny conditions.

Use the format HHHH.HHHHH.

MAC_ACL Specifies the destination host address for which to set permit or deny

conditions. Use the format HHHH.HHHH.

EtherType Specifies the protocol number for which to set the permit or deny conditions.

The range of valid values is from 1536 through 65535.

arp Specifies to permit or deny the Address Resolution Protocol (0x0806).

fcoe Specifies to permit or deny the Fibre Channel over Ethernet Protocol

(0x8906).

ipv4 Specifies to permit or deny the IPv4 protocol (0x0800).

count Enables the counting of the packets matching the rule.

Defaults By default, no MAC ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to insert a rule anywhere in the MAC ACL; it configures rules to match and

permits or drops traffic based on the source and destination MAC addresses, and the protocol type. You can also enable counters for a specific rule. There are 255 ACL counters supported per

port group. Use the no seq value command to remove a rule from the MAC ACL.

Usage Guidelines The first set of [any | host MAC_ACL | MAC_ACL] parameters is specific to the source MAC

address. The second set of [any | host MAC_ACL | MAC_ACL] parameters is specific to the

destination MAC address.

Examples

To create a rule in a MAC extended ACL to permit or drop IPv4 traffic from the source MAC address 0022.3333.4444 to the destination MAC address 0022.3333.5555 and to enable the counting of packets:

switch(conf-macl-ext)#seq 100 deny 0022.3333.4444 0022.3333.5555 ipv4 count
switch(conf-macl-ext)#seq 1000 permit 0022.3333.4444 0022.3333.5555 ipv4
count

To delete a rule from a MAC extended ACL:

switch(conf-macl-ext)#no seq 100

See Also

deny (extended ACLs), deny (extended ACLs), permit (extended ACLs), permit (standard ACLs), resequence access-list mac

seq (standard MAC ACLs)

Inserts a rule anywhere in the MAC ACL.

Synopsis seq value [deny | permit] [any | host MAC _ACL | MAC_ACL] [count]

no seq value

Operands value Specifies the sequence number for the rule. The range of valid values is from

0 through 65535.

permit Specifies rules to permit traffic.

deny Specifies rules to deny traffic.

any Specifies any source MAC address.

host MAC_ACL Specifies the source host MAC address for which to set permit or deny

conditions. Use the format HHHH.HHHH.

MAC_ACL Specifies the destination host MAC address for which to set permit or deny

conditions. Use the format HHHH.HHHHH.

count Enables the counting of the packets matching the rule.

Defaults By default, no MAC ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to configure rules to match and permit or drop traffic based on source and

destination MAC address and protocol type. You can also enable counters for a specific rule. There are 255 ACL counters supported per port group. Use the **no seq** value command to remove a rule

from the MAC ACL.

Usage Guidelines There are no usage guidelines for this command.

Examples To create a rule in a MAC standard ACL to permit or to drop traffic from the source MAC address

0022.3333.4444 and to enable the counting of packets:

switch(conf-macl-std)#seq 100 deny 0022.3333.4444 count
switch(conf-macl-std)#seq 1000 permit 0022.3333.4444 count

To delete a filter rule in a MAC standard ACL:

switch(conf-macl-std)#no seq 100

See Also deny (extended ACLs), deny (extended ACLs), permit (extended ACLs), permit (standard ACLs),

resequence access-list mac

service password-encryption

Configures the username and encrypted password for a user.

Synopsis service password-encryption username password password [encryption-level level]

[role name] [desc description] [enable true | false]

no service password-encryption username

Operands username The user's username. The username must begin with a letter and contain

only letters, numbers, underscores, and periods, with a maximum of 40

characters. The username is case-sensitive.

password The username's password.

password Specifies the user's password.

encryption-level Specifies whether the password is not encrypted (appears in clear text) or

encrypted.

level Specifies whether the password is encrypted. Options include 0 (clear text)

or 7 (encrypted text).

role The roles assigned to the user.

name Specifies the roles that are assigned to the user. The role is optional and, by

default, the user's role is read-only.

desc A description of the user.

description Specifies a description of the user. The text cannot exceed 64 characters.

The text can contain any characters from the printable ASCII character set except for the following: single quote ('), double quote ("), exclamation point

(!), colon (:), and semi-colon (;).

enable Indicates whether a user is enabled or not.

default is true.

Description Use this command to assign encryption attributes for a user's password.

Defaults Clear text (0) is the **encryption-level** default and the default for **enable** is true.

Command Modes Global configuration mode

Using the no form of the service password-encryption command sets the default values of the

individual attributes.

Examples The following example displays how to change a user password from clear text to encrypted text.

switch(config)# username brcdUser role user password "BwrsDbB+tABWGWpINOVKoQ==\"
encryption-level 7 desc "Brocade User" enable true

**

See Also password-attributes, show running-config password-attributes

sflow collector

Identifies the sFlow collectors to which sFlow datagrams are forwarded.

Synopsis sflow collector *ip-address*

no sflow collector ip-address

Operands ip-address Specifies the IP address in the dotted decimal format for the collector.

Defaults There are no defaults for this command.

Command Modes Global configuration mode

Description Use this command to identify the sFlow collectors to which sFlow datagrams are forwarded.

Use the no sflow collector ip-address command to reset the specified collector address to a null

value.

Usage Guidelines You can only specify one sFlow collector.

Examples To identify the sFlow collectors for the IP address 192.10.138.176 to which sFlow datagrams are

forwarded:

switch(config)#sflow collector 192.10.138.176

sflow enable (global version)

Enables sFlow globally.

Synopsis sflow enable

no sflow enable

Operands None

Defaults By default, sFlow is disabled on the system.

Command Modes Global configuration mode

Description Use this command to enable sFlow globally.

Use the no sflow enable command to disable sFlow globally.

Usage Guidelines This command is supported on physical ports only.

Examples To enable sFlow globally:

switch(config)#sflow enable

See Also sflow enable (interface version)

sflow enable (interface version)

Enables sFlow on an interface.

Synopsis sflow enable

no sflow enable

Operands None

Defaults By default, sFlow is disabled on all interfaces.

Command Modes Interface configuration mode

Description Use this command to enable sFlow on an interface.

Use the no sflow enable command to disable sFlow on an interface.

Usage Guidelines This command is supported on physical ports only.

Examples To enable sFlow on an interface:

switch(conf-if-te-0/1)#sflow enable

See Also sflow enable (global version)

sflow polling-interval (global version)

Configures the polling interval globally.

Synopsis sflow polling-interval interval_value

no sflow polling-interval interval_value

Operands interval_value Specifies a value in seconds to set the polling interval. The range of valid

values is from 1 through 65535.

Defaults The default global counter polling interval value is 20 seconds.

Command Modes Global configuration mode

Description Use this command to configure the polling interval globally. The interval is the maximum number

of seconds between successive samples of counters to be sent to the collector.

Use the **no sflow polling interval** *interval_value* command to return to the default value.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the polling interval to 135 seconds:

switch(config)#sflow polling-interval 135

See Also sflow polling-interval (interface version)

sflow polling-interval (interface version)

Configures the polling interval at the interface level.

Synopsis sflow polling-interval interval_value

no sflow polling-interval

Operands interval_value Specifies a value in seconds to set the polling interval. The range of valid

values is from 1 through 65535.

Defaults The default counter polling interval value is 20 seconds.

Command Modes Interface configuration mode

Description Use this command to configure the polling interval for an interface. The interval is the maximum

number of seconds between successive samples of counters to be sent to the collector.

Use the **no sflow polling interval** command to return to the default value.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the polling interval to 135 seconds:

switch(conf-if-te-0/1)#sflow polling-interval 135

See Also sflow polling-interval (global version)

sflow sample-rate (global version)

Sets the number of packets that are skipped before the next sample is taken.

Synopsis sflow sample-rate sample rate

no sflow sample-rate

Operands sample rate Specifies the sampling rate value in packets. The range of valid values is

from 2 through 8388608 packets.

Defaults The default sample rate is 32768 packets.

Command Modes Global configuration mode

Description Use this command to change the current global default sampling rate.

Usage Guidelines Sample-rate is the average number of packets skipped before the sample is taken. sFlow does not

have time-based sampling. If the value entered is not a correct power of 2, the command

generates an error message with the previous and next power-of-2 value. Select one of these two

packet numbers and re-enter the command.

Use the no sflow sample-rate command to return to the default sampling rate.

Examples To change the sampling rate to 4096:

switch(config)#sflow sample-rate 4096

See Also sflow polling-interval (interface version)

sflow sample-rate (interface version)

Sets the number of packets that are skipped before the next sample is taken for a specific

interface.

Synopsis sflow sample-rate sample rate

no sflow sample-rate

Operands sample rate Specifies the sampling rate value in packets. The range of valid values is

from 2 through 8388608.

Defaults The default is the current global default sampling in packets.

Command Modes Interface configuration mode

Description Use this command to change the default sampling rate for a specific interface.

Usage Guidelines This command changes the sampling rate for an interface. By default, the sampling rate of an

interface is set to the same value as the current global default sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next

power-of-2 value. Select one of these two numbers and re-enter the command.

Use the no sflow sample-rate command to return to the default setting.

Examples To change the sampling rate to 4096:

 $switch(\texttt{conf-if-te-0/1}) \\ \# \textbf{sflow sample-rate 4096}$

See Also sflow sample-rate (global version)

2

show accounting logs

Displays the accounting logs.

Synopsis show accounting logs

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display accounting logs.

Usage Guidelines There are no usage guidelines for this command.

Examples switch#show accounting logs

2009/06/24-03:33:45 (UTC), root/root/10.2.2.47/telnet/CLI/Frisco-34, config; rmon

event 15

show arp

Displays the ARP cache.

Synopsis show arp [summary | dynamic | static [summary] | ip ip-address | tengigabit switch/slot/port |

vlan vlan_id | port-channel interface interface-type interface-number]

Operands summary Displays a summary of the ARP table (can be used by itself, or succeed the

static, dynamic or interface keywords).

dynamic Displays all the dynamic ARPs in the ARP table.

static Displays all the static ARPs in the ARP table.

ip Displays the ARP for a particular next-hop.

ip-address Displays the ARP information for this next-hop IP address.

tengigabitethernet Specifies a valid external 10 Gbps Ethernet interface.

switchSpecifies a valid switch number.slotSpecifies a valid slot number.portSpecifies a valid port number.

port-channel interface

Displays the ARP cache for the specified interface only.

interface-type Network interface type (external TenGigabitEthernet interface, null,

port-channel, or VLAN).

interface-number

Layer 2 or Layer 3 Interface number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the contents of the ARP cache.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

show calendar

Displays the current date and time based on the switch hardware clock.

Synopsis show calendar

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the current date and time based on the switch hardware clock.

Usage Guidelines There are no usage guidelines for this command.

Examples To display calendar information:

switch#show calendar

16:33:30 UTC Tue Feb 14 2009

show cee maps

Displays information on the defined CEE maps.

Synopsis show cee maps default

Operands None

Defaults The only map name allowed is "default."

Command Modes Privileged EXEC mode

Description Use this command to display information on the CEE map. The configuration state is displayed with

a list of all of the Layer 2 interfaces bound to the CEE map.

Usage Guidelines Network OS v2.0.0 only allows the CEE map named "default."

Examples None

See Also cee, cee-map (Configuration)

show chassis

Displays all field-replaceable units (FRUs).

Synopsis show chassis [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description

Use this command to display the Field Replaceable Unit (FRU) header content for each object in the chassis. This command displays the following information per line:

- 1. If applicable, the first line displays the chassis backplane version number, in hexadecimal.
- Object type: CHASSIS, FAN, POWER SUPPLY, SW BLADE (switch), WWN (world wide name), or UNKNOWN.
- 3. Object number: Slot nn (for blades), Unit nn (for everything else).
- 4. If the FRU is part of an assembly, a brief description displays in parentheses.
- 5. FRU header version number: Header Version: x
- 6. Value to calculate the object's power consumption: positive for power supplies and negative for consumers. Power Consume Factor: -xxx
- 7. Part number (up to 14 characters): Factory Part Num: xx-xxxxxx-x x
- 8. Serial number (up to 12 characters): Factory Serial Num: xxxxxxxxxx
- 9. FRU manufacture date: Manufacture: Day: dd Month: mm Year: yyyy
- 10. Date of the last FRU header update: Update: Day: dd Month: mm Year: yyyy
- 11. Cumulative time, in days, that the FRU has been powered on: Time Alive:dd days
- 12. Current time, in days, since the FRU was last powered on: Time Awake:dd days
- 13. Externally supplied ID (up to 10 characters): ID: xxxxxxxxxx
- 15. Externally supplied serial number (up to 20 characters): Serial Num: xxxxxxxxxxxxxxxxxxx
- 16. Externally supplied revision number (up to 4 characters): Revision Num: xxxx

The output of this command depends on the platforms on which it is executed. Not all information is available for all platforms. In cases where information is not available, the lines are suppressed.

Usage Guidelines

Pagination is not supported with the all option.

Examples To display the FRU information:

switch#show chassis

switchType: 95

FAN Unit: 2

Time Awake: 4 days

POWER SUPPLY Unit: 2
Header Version: 2
Factory Part Num:

Factory Serial Num:

Manufacture: Day: 28 Month: 6 Year: 2010 Update: Day: 11 Month: 2 Year: 2000

Time Alive: 40 days
Time Awake: 4 days

CHASSIS/WWN Unit: 1
Header Version: 2
Power Consume Factor: 0

Factory Part Num: 40-1000505-07
Factory Serial Num: BKH0322F02B
Manufacture:

Manufacture: Day: 18 Month: 6 Year: 2010 Update: Day: 11 Month: 2 Year: 2000

Time Alive: 70 days
Time Awake: 4 days

2

show clock

Returns the local time, date, and time zone.

Synopsis show clock [switchid switchid | all]

Operands switchid

switchid | all | Specifies the switch ID on which the local time, date, and time zone displays.

Note: For this release, specifying all returns only local information.

Description Use this command to display the current local clock and time zone.

Defaults The local clock is used unless the switch ID or all is specified.

Command Modes Privileged EXEC mode

Usage Guidelines Specify the *all* option to request local clocks from all switches in the cluster.

Examples The following example displays the local time, date, and time on the local clock:

switch# show clock switchid 1

switchid 1:2010-07-21 05:55:14 Etc/GMT

switch# show clock all

switchid 1:2010-07-20 22:55:21 America/Los_Angeles

See Also show diag burninstatus, clock timezone

show debug ip igmp

Displays the IGMP packets received and transmitted, as well as related events.

Synopsis show debug ip igmp

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description This command displays the IGMP packets received and transmitted.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

show debug lacp

Displays the LACP debugging status on the switch.

Synopsis show debug lacp

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the LACP debugging status on the switch.

Usage Guidelines There are no usage guidelines for this command.

Examples None

show debug lldp

Displays the LLDP debugging status on the switch.

Synopsis show debug IIdp

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the LLDP debugging status on the switch.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the LLDP debugging status on the switch:

switch#show debug 1ldp
LLDP debugging status:

Interface te0/0 : Transmit Receive Detail

show debug spanning-tree

Displays the STP debugging status on the switch.

Synopsis show debug spanning-tree

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the STP debugging status on the switch.

Usage Guidelines There are no usage guidelines for this command.

Examples None

show diag burninerrshow

Displays the errors that are stored in the nonvolatile storage on the slot during burn-in.

Synopsis show diag burninerrshow [switchid]

Operands switchid Specifies the switch ID of the switch for which errors stored in the storage on

the slot during burn-in are displayed.

Description Use this command to display errors that are stored in nonvolatile storage on the slot during

burn-in.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display burn-in errors from the switch:

switch# show diag burninerrshow switchid 1

See Also diag burninerrclear, diag clearerror, show diag burninstatus

show diag burninstatus

Displays the diagnostics burn-in status.

Synopsis show diag burninstatus [switchid]

Operands switchid Specifies the switch ID for the switch you want diagnostics burn-in status.

Description Use this command to display the burn-in status for a switch.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display the diagnostics burn-in status:

switch# show diag burninstatus

See Also diag burninerrclear, diag clearerror, show diag burninerrshow

show diag post results

Displays either the brief results or detailed information of the power-on self-test (POST) executed.

Synopsis show diag post results {brief | detailed} [switchid]

Operands brief | detailed Specifies whether the POST passed or failed (brief) or displays detailed

status with the register dump when a POST fails (detailed).

switchid Specifies the switch on which the diagnostic POST results are displayed.

Description Use this command to display either the brief results or details of the last diagnostic POST that was

executed.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display brief POST results (whether the POST passed or failed):

switch(config)# show diag post results brief

See Also diag post

show diag setcycle

Displays the current values used in system verification.

Synopsis show diag setcycle [switchid]

Operands switchid Specifies the switch on which current values are displayed in system

verification.

Description Use this command to display current values used in system verification.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display current values used in system verification:

switch# show diag setcycle switchid 1

See Also diag setcycle

show diag status

Displays the currently running diagnostics tests.

Synopsis show diag status [switchid]

Operands switchid Specifies the switch to display. If not specified, diagnostic tests for all blades

in the system are displayed.

Description Use this command to display currently running diagnostic tests on a specified switch.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To automatically display possible switch IDs in the console:

switch# show diag status switchid 1

See Also show diag post results

2

show dot1x

Displays the overall state of dot1x on the system.

Synopsis show dot1x

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

> Description Use this command to display the overall state of dot1x on the system.

Usage Guidelines There are no usage guidelines for this command.

> **Examples** To display the state of dot1x on the system:

> > switch#show dot1x

802.1X Port-Based Authentication Enabled PAE Capability: Authenticator Only

Protocol Version: Auth Server: RADIUS

RADIUS Configuration

Position: 1

Server Address: 172.21.162.51

Port: 1812

Secret: sharedsecret

Position:

Server Address: 10.32.154.113

1812 Port:

Secret: sharedsecret

show dot1x all

Displays detailed dot1x information for all of the ports.

Synopsis show dot1x all

Operands None

There are no defaults for this command. **Defaults**

Command Modes Privileged EXEC mode

> Use this command to display detailed information for all of the ports. Description

Usage Guidelines There are no usage guidelines for this command.

> **Examples** To display detailed dot1x information for all of the ports:

> > switch#show dot1x all

802.1X Port-Based Authentication Enabled PAE Capability: Authenticator Only

Protocol Version: RADIUS Auth Server:

RADIUS Configuration

Position: 1

Position: Server Address: 172.21.162.51

Port: 1812

Secret: sharedsecret

Position:

Server Address: 10.32.154.113

Port: 1812

Secret: sharedsecret

802.1X info for interface te0/16

Port Control: Auto
Port Auth Status: Unauthorized
Protocol Version: 2

ReAuthentication: Disabled

Auth Fail Max Attempts: 0 ReAuth Max:

Tx Period: 30 seconds Tx Period: 30 seconds
Quiet Period: 60 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 second
PAE State: Connected 3600 seconds PAE State: Connected BE State: Invalid

Supplicant Name:

Supplicant Address: 0000.0000.0000

Current Id: Id From Server:

show dot1x diagnostics interface

Displays all diagnostics information for the authenticator associated with a port.

Synopsis show dot1x diagnostics interface tengigabitethernet slot/port

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number. Specifies a valid port number. port

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

> Description Use this command to display all diagnostics information for the authenticator associated with a

> > port.

Usage Guidelines There are no usage guidelines for this command.

> Examples To display all diagnostics information for the authenticator associated with a port:

> > switch#show dot1x diagnostics interface tengigabitethernet 0/16

802.1X Diagnostics for interface te0/16 authEnterConnecting: 0 authEaplogoffWhileConnecting: 1 authEnterAuthenticating: 0 authSuccessWhileAuthenticating: 0 authTimeoutWhileAuthenticating: 0 authFailWhileAuthenticating: 0 authEapstartWhileAuthenticating: 0 authEaplogoggWhileAuthenticating: 0 authReauthsWhileAuthenticated: 0 authEapstartWhileAuthenticated: 0 authEaplogoffWhileAuthenticated: 0 BackendResponses: 0 BackendAccessChallenges: 0 BackendOtherrequestToSupplicant: 0

BackendAuthSuccess: 0

BackendAuthFails: 0

show dot1x interface

Displays the state of a specified interface.

Synopsis show dot1x interface tengigabitethernet slot/port

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number. Specifies a valid port number. port

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

> Description Use this command to display the state of a specified interface.

Usage Guidelines There are no usage guidelines for this command.

> Examples To display the state of 10 Gbps Ethernet interface 0/16:

switch#show dot1x interface tengigabitethernet 0/16

Dot1x Global Status: Enabled 802.1X info for interface te0/16 _____

Port Control: Auto

Port Auth Status: Unauthorized

Protocol Version: 2
ReAuthentication: Disabled

Auth Fail Max Attempts: 0 ReAuth Max: 2

Tx Period: 30 seconds Tx Period: 30 seconds
Quiet Period: 60 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds PAE State: Connected BE State: Invalid

Supplicant Name:

Supplicant Name: Supplicant Address: 0000.0000.0000

Current Id: Id From Server:

show dot1x session-info interface

Displays all statistical information of an established session.

Synopsis show dot1x session-info interface [tengigabitethernet slot/port]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to display all statistical information of the established session for a specified

interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To display all statistical information of the established session:

switch#show dot1x session-info interface tengigabitethernet 0/16

802.1X Session info for te0/16

User Name: testuser
Session Time: 3 mins 34 secs
Terminate Cause: Not terminated yet

show dot1x statistics interface

Displays the statistics of a specified interface.

Synopsis show dot1x statistics interface interface [tengigabitethernet slot/port]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the statistics of a specified interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the statistics for 10 Gbps Ethernet interface 0/16:

802.1% statistics for interface te0/16

switch#show dot1x statistics interface tengigabitethernet 0/16

EAPOL Frames Rx: 0 - EAPOL Frames Tx: 0

EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0

EAP Rsp/Id Frames Rx: 2 - EAP Response Frames Rx: 10

EAP Req/Id Frames Tx: 35 - EAP Request Frames Tx: 0

Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0

EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src: 0000.0000.0000

show dpod

Displays Dynamic Ports on Demand (POD) license information.

Synopsis show dpod

Operands None

Defaults None

Command Modes Privileged EXEC mode

> Use this command to display Dynamic POD license information for the local switch. Description

Usage Guidelines This command is not supported in VCS mode.

> Examples To display Dynamic POD assignment information:

```
switch# show dpod
```

24 ports are available in this switch

1 POD license is installed

Dynamic POD method is in use

24 port assignments are provisioned for use in this switch:

16 port assignments are provisioned by the base switch license

8 port assignments are provisioned by the first POD license

0 more assignments are added if the second POD license is installed

21 ports are assigned to installed licenses:

16 ports are assigned to the base switch license

5 ports are assigned to the first POD license

Ports assigned to the base switch license:

Te 0/1, Te 0/10, Te 0/11, Te 0/12, Te 0/13, Te 0/14, Te 0/15, Te 0/16, Te

0/17, Te 0/18, Te 0/19, Te 0/20, Te 0/21, Te 0/22, Te 0/23, Te 0/24

Ports assigned to the first POD license:

Te 0/5, Te 0/6, Te 0/7, Te 0/8, Te 0/9

Ports assigned to the second POD license:

None

Ports not assigned to a license:

Te 0/2, Te 0/3, Te 0/4

3 license reservations are still available for use by unassigned ports

See Also dpod, show running-config dpod

show environment

Displays fan, temperature, redundant power system (RPS) availability, and power information for the switch.

Synopsis show environment

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display fan, temperature, redundant power system (RPS) availability, and

power information for the switch.

Usage Guidelines There are no usage guidelines for this command.

Examples To display both fan and temperature environmental status:

switch#show environment

-- Fan Status -Fan 1 is Ok
Fan 2 is Ok
Fan 3 is Ok
-- Power Supplies -PSO is OK

PS1 is faulty

-- Unit Environment Status --Sensor State Centigrade Fahrenheit ID _____ 1 Ok 44 111 2 Ok 40 104 3 Ok 47 116 Ok 32 89

show environment fan

Displays fan status information.

Synopsis show environment fan [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display fan status information. The fan status information includes the

following values:

OK Fan is functioning correctly at the displayed speed (RPM).

absent Fan is not present.

below minimum Fan is present but rotating too slowly or stopped.

above minimum Fan is rotating too quickly.
unknown Unknown fan unit installed.

faulty Fan has exceeded hardware tolerance and has stopped. In this case, the last

known fan speed is displayed.

Airflow direction Port side intake or Port side exhaust.

Usage Guidelines Pagination is not supported with the **all** option.

Examples To display the fan status information on the local switch:

switch# show environment fan

show environment fan

Fan 1 is Ok, speed is 2057 RPM
Fan 2 is Ok, speed is 2009 RPM
Fan 3 is Ok, speed is 2045 RPM
Airflow direction: Port side intake

See Also show environment history, show environment power, show environment sensor, show environment

temp

show environment history

Displays the field-replaceable unit (FRU) history log.

Synopsis show environment history [switchid {switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the history log, which records insertion and removal events for

field-replaceable units (FRUs), such as blades, power supplies, fans, and world wide name (WWN) cards. The type of FRU supported depends on the hardware platform. The command output

includes the following information:

Object type On standalone platforms: FAN, POWER SUPPLY, WWN (WWN card), or

UNKNOWN.

On enterprise-class platforms: CHASSIS, FAN, POWER SUPPLY, SW BLADE (port blade), CP BLADE (control processor), WWN (WWN card), or UNKNOWN.

Object number Displays the slot number for blades. Displays the unit number for all other

object types.

Event type Displays Inserted, Removed, or Invalid

Time of the event Displays the date in the following format: Day Month dd hh:mm:ss yyyy.

Factory Part Number

Displays the part number (xx-yyyyyyy-zz) or Not available.

Factory Serial Number

Displays the switch serial number (xxxxxxxxxxxx) or Not available.

Usage Guidelines Pagination is not supported with the **all** option.

Examples To display the FRU history:

switch# show environment history

FAN Unit 1 Inserted at Wed Jun 30 15:34:56 2010

Factory Part Number: Not Available Factory Serial Number: Not Available

FAN Unit 2 Inserted at Wed Jun 30 15:34:56 2010

Factory Part Number: Not Available Factory Serial Number: Not Available

POWER SUPPLY Unit 1 Inserted at Wed Jun 30 15:34:56 2010

Factory Part Number: Not Available Factory Serial Number: Not Available

2

POWER SUPPLY Unit 2 Inserted at Wed Jun 30 15:34:56 2010 Factory Part Number: Not Available

Factory Serial Number: Not Available

Records: 4

See Also

show environment fan, show environment power, show environment sensor, show environment temp

show environment power

Displays power supply status.

Synopsis show environment power [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of the switch power supplies. The status can be

one of the following values:

OK Power supply is functioning correctly.

absent Power supply is not present.

unknown Unknown power supply unit is installed.

predicting failure Power supply is present but predicting failure.

faulty Power supply is present but faulty (no power cable, power switch turned off,

fuse blown, or other internal error).

Usage Guidelines Pagination is not supported with the **all** option.

Examples To display the power supply status:

switch# show environment power

Power Supply #1 is absent Power Supply #2 is OK

See Also show environment fan, show environment history, show environment sensor, show environment

temp

show environment sensor

Displays the environment sensor status.

Synopsis show environment sensor [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current temperature, fan, and power supply status readings from

sensors located on the switch.

Usage Guidelines Pagination is not supported with the **all** option.

Examples To display the sensor readings on the switch:

```
switch# show environment sensor
sensor 1: (Temperature ) is Ok, value is 36 C
sensor 2: (Temperature ) is Ok, value is 40 C
sensor 3: (Temperature ) is Ok, value is 32 C
sensor 4: (Fan ) is Absent
sensor 5: (Fan ) is Ok, speed is 7345 RPM
sensor 6: (Power Supply) is Absent
sensor 7: (Power Supply) is Ok
```

See Also

show environment fan, show environment history, show environment power, show environment

temp

show environment temp

Displays environment temperature.

Synopsis show environment temp [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current temperature readings of all temperature sensors in a

switch. For each sensor, this command displays the following information:

slot number (if applicable), the sensor state, and the temperature. The temperature readings are

given in both Centigrade and Fahrenheit.

Usage Guidelines Pagination is not supported with the **all** option.

Refer to the hardware reference manual for your switch to determine the normal temperature

range.

Examples To display the temperature readings on the switch:

switch#	show environmen	nt temp	
Sensor	State	Centigrade	Fahrenheit
ID			
======		.========	========
1	Ok	36	96
2	Ok	40	104
3	Ok	32	89

See Also show environment fan, show environment history, show environment power, show environment

sensor

show fabric all

Displays the VCS fabric membership information.

NOTE

The **show vcs** command returns the state as "disabled" if the switch is in standalone mode. The **show fabric all** command cannot be issued in standalone mode.

Synopsis show fabric all

Operands None

Description Use this command to display information about the fabric.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display the VCS fabric information:

switch# show fabric all

VCS Id: 1

VCS Mode: Fabric Cluster

RBridge-ID	WWN	IP Address	Name
1	10:00:00:05:1E:CD:44:6A	10.17.87.144	"RB1"
2	10:00:00:05:1E:CD:42:6A	10.17.87.145	"RB2"
3	10:00:00:05:1E:CD:55:6A	10.17.87.155	"RB3"
4	10:00:00:05:1E:CD:42:EA	10.17.87.156	"RB4"
5	10:00:00:05:1E:CD:52:6A	10.17.87.157	"RB5"
6	10:00:00:05:1E:CD:53:6A	10.17.87.158	"RB6"
10	10:00:00:05:33:13:6A:BE	10.17.87.169	"RB10"
11	10:00:00:05:1E:CD:38:6A	10.17.86.240	"RB11"
12	10:00:00:05:1E:CD:3F:EA	10.17.86.241	>"RB12-a"

Note The angle bracket (>), as shown with RBridge-ID 12-a, indicates the principal switch.

See Also

diag post, fabric route multicast, fabric trunk enable, show diag burninstatus, show diag burninstatus, show fabric route multicast, show fabric route topology, show fabric trunk

show fabric isl

Displays inter-switch link (ISL) information in the fabric.

Synopsis show fabric isl [rbridgeld id | all]

Operands rbridge-id Specifies the ID of the routing bridge. Only the local RBridge can be selected.

only local information.

Description Use this command to display ISL information in the fabric.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples The following example displays inter-switch link (ISL) information in the fabric.

switch# show fabric isl rbridgeID 1

RBridge-ID: 1 #ISLs: 11

Src-Port	Nbr-Port	Nbr-WWN	BW	Trunk	Nbr-Name
Te 1/0/2	Te 21/0/56	10:00:00:05:33:13:5F:	BE 60G	Yes	"Edget12r1_1_21"
Te 1/0/7	Te 22/0/55	10:00:00:05:33:40:31	93 400	Yes	"Edget12r12_22"
Te 1/0/12	Te 22/0/60	10:00:00:05:33:40:31	93 200	Yes	"Edget12r12_22"
Te 1/0/15	Te 23/0/57	10:00:00:05:33:13:55	BE 60G	Yes	"Edget12r21_23"
Te 1/0/20	Te 24/0/56	10:00:00:05:33:13:61	BE 10G	Yes	"Edget12r22_24"
Te 1/0/22	Te 24/0/58	10:00:00:05:33:13:61	BE 40G	Yes	"Edget12r22_24"
Te 1/0/26	Te 25/0/56	10:00:00:05:33:40:2F	C9 60G	Yes	"Edget12r31_25"
Te 1/0/34	Te 26/0/58	10:00:00:05:33:41:1E	B7 60G	Yes	"Edget12r32_26"
Te 1/0/37	Te 27/0/56	10:00:00:05:33:40:42	43 400	Yes	"Edget12r41_27"
Te 1/0/41	Te 27/0/59	10:00:00:05:33:40:42	43 200	Yes	"Edget12r41_27"
Te 1/0/44	Te 28/0/56	10:00:00:05:33:40:38	3B 60G	Yes	"Edget12r42_28"

See Also fabric isl enable, show diag burninstatus

show fabric islports

Displays information for all inter-switch link (ISL) ports in the switch.

Synopsis show fabric islports [rbridgeld id]

Operands rbridgeld Specifies the ID of the routing bridge. Only the local RBridge can be selected.

id Specifies the ID of the routing bridge on which the ISL ports are displayed.

Description Use this command to display information for all ISL ports in the switch.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode.

Usage Guidelines There are no usage guidelines for this command.

Examples To display information for all ISL ports in the core switch:

```
switch# show fabric islports rbridgeId 1 core switch
              switch2_1_1
 Name:
              97.2
 Type:
              Online
 State:
 Role:
              Fabric Subordinate
 VCS Id:
 VCS Mode: Fabric Cluster
 RBridge-ID: 1
              10:00:00:05:33:13:50:be
 WWN:
              00:05:33:13:50:be
 FCF MAC:
Port State
                     Operational State
    1/0/1 Up
                 ISL Trunk port, Primary is Te 1/0/2
                 ISL 10:00:00:05:33:13:5f:be "Edget12r1_1_21" (downstream)(Trunk
    1/0/2 Up
                     Primary)
    1/0/3 Up
Te
                 ISL Trunk port, Primary is Te 1/0/2
    1/0/4 Up
                 ISL Trunk port, Primary is Te 1/0/2
Te
    1/0/5 Up
                 ISL Trunk port, Primary is Te 1/0/2
Te
Te
    1/0/6 Up
                 \mathsf{ISL} Trunk port, Primary is Te 1/0/2
    1/0/7 Up
                 ISL 10:00:00:05:33:40:31:93 "Edget12r12_22" (Trunk Primary)
Te
    1/0/8 Up
                 ISL Trunk port, Primary is Te 1/0/7
Te
    1/0/9 Up
                 \mathsf{ISL} Trunk port, Primary is Te 1/0/7
Te
    1/0/10 Up
                 ISL Trunk port, Primary is Te 1/0/7
Te
    1/0/11 Up
                 ISL Trunk port, Primary is Te 1/0/12
Te
    1/0/12 Up
                 ISL 10:00:00:05:33:40:31:93 "Edget12r12_22" (Trunk Primary)
Te
    1/0/13 Up
                 ISL Trunk port, Primary is Te 1/0/15
Te
    1/0/14 Up
                 ISL Trunk port, Primary is Te 1/0/15
Te
    1/0/15 Up
                 ISL 10:00:00:05:33:13:55:be "Edget12r21_23" (downstream)(Trunk
Te
                     Primary)
Te
    1/0/16 Up
                 ISL Trunk port, Primary is Te 1/0/15
Te
    1/0/17 Up
                 ISL Trunk port, Primary is Te 1/0/15 )
Te
    1/0/18 Up
                 ISL Trunk port, Primary is Te 1/0/15)
Te
   1/0/19 Down
                 ISL 10:00:00:05:33:13:61:be "Edget12r22_24" (Trunk Primary)
Te 1/0/20 Up
                 ISL Trunk port, Primary is Te 1/0/22
Te 1/0/21 Up
                 ISL 10:00:00:05:33:13:61:be "Edget12r22_24" (Trunk Primary)
Te 1/0/22 Up
Te 1/0/23 Up
                 ISL Trunk port, Primary is Te 1/0/22
Te 1/0/24 Up
                 ISL Trunk port, Primary is Te 1/0/22
```

```
Te
    1/0/25 Up
                ISL Trunk port, Primary is Te 1/0/26
Te
    1/0/26 Up
                ISL 10:00:00:05:33:40:2f:c9 "Edget12r31_25" (Trunk Primary)
Te
    1/0/27 Up
                ISL Trunk port, Primary is Te 1/0/26
Te
   1/0/28 Up
                ISL Trunk port, Primary is Te 1/0/26
   1/0/29 Up
Te
                ISL Trunk port, Primary is Te 1/0/26
Te
   1/0/30 Up
                ISL Trunk port, Primary is Te 1/0/26
   1/0/31 Up
Te
                ISL Trunk port, Primary is Te 1/0/34
   1/0/32 Up
Te
                ISL Trunk port, Primary is Te 1/0/34
    1/0/33 Up
                ISL Trunk port, Primary is Te 1/0/34
Te
    1/0/34 Up
                ISL 10:00:00:05:33:41:1e:b7 "Edget12r32_26" (upstream)(Trunk Primary)
Te
Te
    1/0/35 Up
                ISL Trunk port, Primary is Te 1/0/34
Te
    1/0/36 Up
                ISL Trunk port, Primary is Te 1/0/34
Te
    1/0/37 Up
                ISL 10:00:00:05:33:40:42:43 "Edget12r41_27" (Trunk Primary)
Te
    1/0/38 Up
                ISL Trunk port, Primary is Te 1/0/37
Te
    1/0/39 Up
                ISL Trunk port, Primary is Te 1/0/37
Te
    1/0/40 Up
                ISL Trunk port, Primary is Te 1/0/37
Te
    1/0/41 Up
                ISL 10:00:00:05:33:40:42:43 "Edget12r41_27" (Trunk Primary)
Te
    1/0/42 Up
                ISL Trunk port, Primary is Te 1/0/41
Te
   1/0/43 Up
                ISL Trunk port, Primary is Te 1/0/44
Te
   1/0/44 Up
                ISL 10:00:00:05:33:40:38:3b "Edget12r42_28" (Trunk Primary)
   1/0/45 Up
Te
                ISL Trunk port, Primary is Te 1/0/44
   1/0/46 Up
Te
                ISL Trunk port, Primary is Te 1/0/44
   1/0/47 Up
Te
                ISL Trunk port, Primary is Te 1/0/44
   1/0/48 Up
Te
                ISL Trunk port, Primary is Te 1/0/44
   1/0/49 Up
                ISL Down
Te
                ISL Down
Te 1/0/50 Up
                ISL Down
Te 1/0/51 Up
                ISL Down
Te 1/0/52 Up
                ISL Down
Te 1/0/53 Up
Te 1/0/54 Up
                ISL Down
Te 1/0/55 Up
                ISL Down
Te 1/0/56 Up
                ISL Down
Te 1/0/57 Up
                ISL Down
                ISL Down
Te 1/0/58 Up
Te 1/0/59 Up
                ISL Down
Te 1/0/60 Up
                ISL Down
```

See Also fabric isl enable, show diag burninstatus

show fabric route multicast

Displays ISLs that any received broadcast, unknown unicast, and multicast (BUM) traffic will forward.

Synopsis show fabric route multicast [rbridgeld id | all]

Operands rbridgeld Specifies the ID of the routing bridge.

in this release.

Description Use this command to display the multicast routing information for all ports in the switch. The

multicast routing information indicates all ports that are members of the multicast distribution

tree: ports that are able to send and receive multicast frames.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display the multicast routing information for all ports in the switch:

switch# show fabric route multicast rbridgeID 1

Root of the Multicast-Tree

Domain: 1

Mcast Priority: 0

Enet IP Addr: 10.20.61.1
WWN: 10:00:00:05:33:13:50:be

Name: AggT12_1_1

RBridge-ID: 1

Src-Port	Nbr-Port	BW	Trunk
Te 1/0/2	Te 21/0/56	60G	Yes
Te 1/0/7	Te 22/0/55	40G	Yes
Te 1/0/15	Te 23/0/57	60G	Yes
Te 1/0/22	Te 24/0/58	40G	Yes
Te 1/0/26	Te 25/0/56	60G	Yes
Te 1/0/34	Te 26/0/58	60G	Yes
Te 1/0/41	Te 27/0/59	20G	Yes
Te 1/0/44	Te 28/0/56	60G	Yes

From the edge switch:

Te 1/0/23 Te 7/0/37

switch# show fabric route multicast

```
Root of the Multicast-Tree
_____
Domain: 1
Mcast Priority: 0
Enet IP Addr: 10.20.51.60
WWN: 10:00:00:05:1e:cd:79:7a
Name: C24_60
RBridge-ID: 1
Src-Port
        Nbr-Port
                     BW
                           Trunk
Te 1/0/2 Te 4/0/18
                     10G
                           Yes
Te 1/0/4 Te 5/0/4
                     10G
                           Yes
Te 1/0/5 Te 3/0/13
                    10G
                           Yes
Te 1/0/7 Te 6/0/15
                     30G
                           Yes
Te 1/0/15 Te 2/0/9
                     20G
                           Yes
```

See Also fabric route multicast, show fabric route topology, show running-config fabric route mcast

Yes

10G

show fabric route topology

Displays the RBridge routes from the source switch to the destination switch.

Synopsis show fabric route topology [src-rbridgeld src_id] [dst-rbridgeld dst_id]

NOTE

The source RBridge ID must be the local RBridge ID in this release. It is an optional operand. If you do not specify the source RBridge ID or the destination RBridge ID, the system routes to all destinations in the Fabric.

Operands src-rbridgeld The source routing bridge (RBridge)

src-id Specifies details on the source RBridge.

dst-rbridgeld The destination RBridge.

dst_id Specifies details on the destination RBridge.

Description Use this command to display the Rbridge routes to other switches.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines The RBridge routes to other switches are the available paths to remote domains that unicast

traffic can take.

Examples To display the fabric route topology information:

switch# show fabric route topology

Total Path Count: 22

Src-ID	Dst-ID	OutPort	-	Cost	Nbr-Port	BW	Trunk
1	2	Te 1/0/2		1000	Te 21/0/56	60G	Yes
	2	Te 1/0/26	2	1000	Te 25/0/56	60G	Yes
	2	Te 1/0/44	2	1000	Te 28/0/56	60G	Yes
	2	Te 1/0/15	2	1000	Te 23/0/57	60G	Yes
	2	Te 1/0/34	2	1000	Te 26/0/58	60G	Yes
	2	Te 1/0/7	2	1000	Te 22/0/55	40G	Yes
	2	Te 1/0/22	2	1000	Te 24/0/58	40G	Yes
	2	Te 1/0/37	2	1000	Te 27/0/56	40G	Yes
	2	Te 1/0/12	2	1000	Te 22/0/60	20G	Yes
	2	Te 1/0/41	2	1000	Te 27/0/59	20G	Yes
	2	Te 1/0/20	2	1000	Te 24/0/56	10G	Yes
	21	Te 1/0/2	1	500	Te 21/0/56	60G	Yes
	22	Te 1/0/7	1	500	Te 22/0/55	40G	Yes
	22	Te 1/0/12	1	500	Te 22/0/60	20G	Yes
	23	Te 1/0/15	1	500	Te 23/0/57	60G	Yes
	24	Te 1/0/22	1	500	Te 24/0/58	40G	Yes
	24	Te 1/0/20	1	500	Te 24/0/56	10G	Yes
	25	Te 1/0/26	1	500	Te 25/0/56	60G	Yes
	26	Te 1/0/34	1	500	Te 26/0/58	60G	Yes
	27	Te 1/0/37	1	500	Te 27/0/56	40G	Yes
	27	Te 1/0/41	1	500	Te 27/0/59	20G	Yes

See Also fabric route multicast

show fabric trunk

Displays interswitch (ISL) trunk information.

Synopsis show fabric trunk [rbridgeld | all]

Operands rbridgeld | all Displays trunk details on the specified routing bridge (RBridge).

Description Use this command to display trunking information of ISL ports.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display the fabric trunk information:

switch# show fabric trunk rbridgeId 12

RBridge-ID: 12

Group	Src-Port	Nbr-Port	Nbr-WWN
1	te12/0/1	te3/0/13	10:00:00:05:1E:CD:55:6A
1	te12/0/2	te3/0/14	10:00:00:05:1E:CD:55:6A
2	te12/0/3	te1/0/13	10:00:00:05:1E:CD:44:6A
2	te12/0/4	te1/0/14	10:00:00:05:1E:CD:44:6A
3	te12/0/6	te6/0/14	10:00:00:05:1E:CD:53:6A
3	te12/0/5	te6/0/13	10:00:00:05:1E:CD:53:6A
4	te12/0/9	te4/0/13	10:00:00:05:1E:CD:42:EA
4	te12/0/10	te4/0/14	10:00:00:05:1E:CD:42:EA
5	te12/0/12	te2/0/14	10:00:00:05:1E:CD:42:6A
5	te12/0/11	te2/0/13	10:00:00:05:1E:CD:42:6A
7	te12/0/18	te5/0/14	10:00:00:05:1E:CD:52:6A
7	te12/0/17	te5/0/13	10:00:00:05:1E:CD:52:6A
8	te12/0/22	te240/0/14	10:00:00:05:1E:CD:63:6A
8	te12/0/21	te240/0/13	10:00:00:05:1E:CD:63:6A

See Also fabric trunk enable

show fcoe fabric-map

Displays the current configuration of the FCoE fabric-map.

Synopsis show fcoe fabric-map

Operands None

Defaults There are no default guidelines.

Command Modes Privileged EXEC mode

Description This command displays the current configuration of the FCoE fabric-map.

Usage Guidelines There are no usage guidelines for this command.

Examples switch#show fcoe fabric-map

Fabric-Map VLAN VFID Pri FCMAP FKA Timeout

default 1002[D] 128[D] 3[D] 0xefc00[D] 8000[D] Enabled[D]

Total number of Fabric Maps = 1

show fcoe interface

Displays a synopsis of the FCoE interfaces.

Synopsis show fcoe interface [brief | interface fcoe switch/slot/port]

Operands brief Displays a brief synopsis of the configuration status

interface fcoe The VN number/VCS node mapped ID/logical port number for the

virtual-fabric.

switch Specifies the switch. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults The only map name allowed is "default."

Command Modes Privileged EXEC mode

Description This command displays a synopsis of the configuration status of all FCoE interfaces.

Usage Guidelines There are no usage guidelines for this command.

Examples None

show fcoe login

Displays FCoE login information.

Synopsis show fcoe login

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description This command displays FCoE login information.

Usage Guidelines There are no usage guidelines for this command.

Examples None

2

show fcoe map

Displays all FCoE maps, or a single map.

Synopsis show fcoe map

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description This command displays all available FCoE maps, or a single designated map. However, for Network

OS v2.0.0, the only map name allowed is "default."

Usage Guidelines There are no usage guidelines for this command.

Examples switch#show fcoe map default

Name DCB-Map FABRIC-MAP(s)

default default default

show file

Displays the contents of a file.

Synopsis show file file

Operands file Specifies the name of the file to be displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the contents of a file in the local flash memory.

Usage Guidelines This command is supported only on the local switch.

Examples To display the contents of the startup configuration file:

```
switch# show file startup-config
logging switchid 2
raslog console INFO
logging syslog ipaddress [ ]
switch-attributes 2
chassis-name chassis
host-name sw
support switchid 2
ffdc
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr
 rw
!
snmp-server community "Secret COde"
snmp-server community common
snmp-server community private
[output truncated]
```

See Also

copy, copy running-config startup-config, delete, dir, chassis disable, show running-config, show support, vcs

show firmwaredownloadstatus

Displays the firmware download activity log.

Synopsis show firmwaredownloadstatus [brief][switchid {switchid | all }]

Operands brief Displays the end result and time stamp only.

switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchid Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display an event log that records the progress and status of events that

occur during a firmware download. The event log is created by the current **firmware download** command and is kept until another **firmware download** command is issued. There is a time stamp

associated with each event.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the firmware download event log on the local switch:

switch#show firmwaredownloadstatus

```
[1]: Tue Sep 21 18:54:08 2010
```

Firmware is being downloaded to the switch. This step may take up to 30 minutes.

[2]: Tue Sep 21 18:59:20 2010

Firmware has been downloaded to the secondary partition of the switch.

[3]: Tue Sep 21 19:02:10 2010

The firmware commit operation has started. This may take up to $10\ \text{minutes}$.

[4]: Tue Sep 21 19:04:47 2010

The commit operation has completed successfully.

[5]: Tue Sep 21 19:04:47 2010

Firmwaredownload command has completed successfully. Use 'show version' to verify the firmware versions.

To display the firmware download end result and time stamp only:

switch#show firmwaredownloadstatus brief

[5]: Tue Sep 21 19:04:47 2010

Firmwaredownload command has completed successfully. Use 'show version' to verify the firmware versions.

See Also vcs, firmware download, firmware restore, show version

show interface

Synopsis show interface [port-channel number | tengigabitethernet slot/port | switchport |

tracked | fcoe switch/slot/port | vlan vlan_id]

Operands port-channel number

Specifies to display the port-channel number. The range of valid values is

from 1 through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

switchport Specifies to display information for Layer 2 interfaces.

tracked Displays the tracked status of the interface.

fcoe switch/slot/port

Displays the FCoE informtation for the designated interface.

vlan *vlan_id* Specifies which VLAN interface to display. The range of valid values is from 1

through 3583.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the detailed interface configuration and capabilities of all interfaces

or for a specific interface. The **show interface** command displays all available information.

Usage Guidelines There are no usage guidelines for this command.

Examples To display detailed information for 10 Gbps Ethernet interface 0/1:

```
switch#show interface tengigabitethernet 0/1
```

```
TenGigabitEthernet 0/1 is admin down, line protocol is down (admin down)
Hardware is Ethernet, address is 0005.1e76.1aa5
    Current address is 0005.1e76.1aa5
Pluggable media present, Media type is sfp
    Wavelength is 850 nm
Interface index (ifindex) is 67174401
MTU 2500 bytes
LineSpeed: 10000 Mbit, Duplex: Full
Flowcontrol rx: on, tx: on
Last clearing of show interface counters: 00:02:18
Queueing strategy: fifo
Receive Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Broadcasts: 0
    64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
    Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    0 packets, 0 bytes
```

```
Unicasts: 0, Multicasts: 0, Broadcasts: 0
Underruns: 0
Errors: 0, Discards: 0
Rate info (interval 299 seconds):
Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:02:17
```

To display Layer 2 information for all interfaces:

switch#show interface switchport

```
Interface name
                          : TenGigabitEthernet 0/8
Interface name : TenGiga
Switchport mode : access
Ingress filter : enable
Acceptable frame types : all
Default Vlan : 1
                          : 1
Active Vlans
Inactive Vlans
                          : -
Interface name : TenGigabitEthernet 0/19
Switchport mode : hybrid
Ingress filter : enable
Acceptable frame types : all
Default Vlan : 1
                          : 1
Active Vlans
Inactive Vlans
                         : 100
Interface name : TenGigabitEthernet 0/20
Switchport mode : trunk
Ingress filter : enable
Acceptable frame types : vlan-tagged only
Default Vlan : 0
Active Vlans
                          : 1
```

: -

See Also show ip interface

Inactive Vlans

show interface management

Displays the management interfaces.

Synopsis show interface management [switchID/0]

Operands switchID/O Specifies the switch management interface.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the management interfaces.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the management interface on the local switch:

```
switch# show interface management
Management 2/0
ip address 10.20.49.112/20
ip gateway-address 10.20.48.1
ipv6 ipv6_address [ ]
ipv6 ipv6_gateways [ fe80::21b:edff:fe0b:2400 ]
LineSpeed Actual "1000 Mbit, Duplex: Full"
LineSpeed Configured "Auto, Duplex: Full"
```

See Also interface management, show running-config interface management

2

show ip fib

Displays the FIB information.

Synopsis show ip fib IPv4_address IPv4_prefix_IP_length

Operands *IPv4_address* The IPv4 32-bit (four-byte) address.

IPv4_prefix_IP_length

The IPv4 routing prefix.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the FIB information.

Usage Guidelines There are no usage guidelines for this command.

Examples switch#show ip fib 4.4.4.0

 Destination
 NextHop(s)
 Interface
 ECMP
 Mac-address

 4.4.4.0/24
 Connected
 Te 0/15
 No 0000.0000.0000

 4.4.4.1/32
 Receive
 Te 0/15
 No 0000.0000.0000

Number of ARPs in FIB : 0 Number of Routes in FIB : 2

See Also show ip forwarding, show ip fib, clear ip fib

show ip forwarding

Displays the status of IP forwarding.

Synopsis show ip forwarding

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the status of IP forwarding.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also show ip interface, show ip fib, show ip fib

show ip igmp groups

Displays information related to learned groups in the IGMP protocol module.

Synopsis show ip igmp groups [A.B.C.D | detail [[interface tengigabitethernet slot/port | detail] | [interface

vlan vlan_id | detail] | [interface port-channel number | detail]]]

Operands A.B.C.D Specifies the group address, as a subnet number in dotted decimal format

(for example, 10.0.0.1), as the allowable range of addresses included in the

multicast group.

detail Displays the IGMPv3 source information.

interface Use this keyword to specify any of the following interfaces:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

detail Displays the IGMPv3 source information.

interface Use this keyword to specify any of the following interfaces:

vlan vlan id Specifies which VLAN interface to display the snooping configuration related

information. The range of valid values is from 1 through 3583.

detail Displays the IGMPv3 source information.

interface Use this keyword to specify any of the following interfaces:

port-channel number

Specifies the interface is a port-channel. The range of valid values is from 1 through 63 for standalone mode. The range of valid values is from 1 through

6144 for VCS mode.

detail Displays the IGMPv3 source information.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the IGMP database, including configured entries for either all groups

on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

Usage Guidelines The remote rbridge information is not displayed when the detail and interface operands are

used.

Examples None

show ip igmp snooping

Displays IGMP snooping information.

Synopsis show ip igmp snooping [[interface vlan vlan_id | mrouter interface vlan vlan_id]]

Operands interface vlan vlan_id

Specifies which VLAN interface to display the snooping configuration related

information. The range of valid values is from 1 through 3583.

mrouter interface vlan vlan_id

Specifies which VLAN interface to display the snooping configuration related

information. The range of valid values is from 1 through 3583.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description Use this command to display IGMP snooping information, display multicast router port related

information for the specified VLAN, or to display snooping statistics for the specified VLAN in the

IGMP protocol module.

Usage Guidelines There are no usage guidelines for this command.

Examples To display IGMP snooping information for VLAN 5:

 $\verb|switch#show ip igmp snooping interface vlan 5|\\$

show ip interface

Displays the IP interface status and configuration of all interfaces or a specified interface.

Synopsis show ip interface [brief | port-channel number brief | tengigabitethernet slot/port brief | vlan

vlan_id brief]

Operands brief Specifies to display a brief summary of the IP status and configuration.

port-channel number

Specifies to display the port-channel number. The range of valid values is

from 1 through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

vlan vlan_id Specifies to display a the VLAN number. The range of valid values is from 1

through 3583.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display IP interface status and configuration of all interfaces or a specified

interface.

Usage Guidelines There are no usage guidelines for the command.

Examples To display information about all of the interfaces in the summary format:

switch#show ip interface brief

Interface		IP-Address	Status	Protocol
======		=======	=====	======
Port-channel 10		unassigned	up	down
Port-channel 11		unassigned	up	down
Port-channel 12		unassigned	up	down
Port-channel 13		unassigned	up	up
Port-channel 14		unassigned	up	down
Port-channel 15		unassigned	up	up
TenGigabitEthernet	0/0	unassigned	up	up
TenGigabitEthernet	0/1	unassigned	up	down
TenGigabitEthernet	0/2	unassigned	up	up
TenGigabitEthernet	0/3	unassigned	up	up
TenGigabitEthernet	0/4	unassigned	up	down
TenGigabitEthernet	0/5	unassigned	up	down
TenGigabitEthernet	0/6	unassigned	up	down
TenGigabitEthernet	0/7	unassigned	up	up
TenGigabitEthernet	0/8	unassigned	up	up
TenGigabitEthernet	0/9	unassigned	up	up
TenGigabitEthernet	0/10	unassigned	up	down
TenGigabitEthernet	0/11	unassigned	up	down
TenGigabitEthernet	0/12	unassigned	up	up
TenGigabitEthernet	0/13	unassigned	up	up
TenGigabitEthernet	0/14	unassigned	up	down

TenGigabitEthernet	0/15	unassigned	up	up
TenGigabitEthernet	0/16	unassigned	up	down
TenGigabitEthernet	0/17	unassigned	up	up
TenGigabitEthernet	0/18	unassigned	up	down
TenGigabitEthernet	0/19	unassigned	up	up
TenGigabitEthernet	0/20	unassigned	up	up
TenGigabitEthernet	0/21	unassigned	up	up
TenGigabitEthernet	0/22	unassigned	up	up
TenGigabitEthernet	0/23	unassigned	up	up
Vlan 1		unassigned	administratively down	down
Vlan 100		unassigned	administratively down	down
Vlan 200		unassigned	administratively down	down

See Also show interface

show lacp counter

Displays the Link Aggregation Control Protocol (LACP) counters on all port-channels or a specified

interface.

Synopsis show lacp counter number

Operands *number* Specifies the port-channel number to display. The range of valid values is

from 1 through 63.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the LACP packet counters on all interfaces that belong to a

port-channel or a specific interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To show the LACP counters for port-channel 10:

switch#show lacp counter 10

% Traffic statistics

Port	LAC	PDUs	Mar	ker	Pckt	err
	Sent	Recv	7 Sent	Recv	Sent	Recv
% Aggre	egator	Po 10	1000000			
Te 0/1	65	0	0	0		0 0
Te 0/2	64	0	0	0		0 0
Te 0/3	64	0	0	0		0 0
Te 0/4	0	0	0	0		0 0
switch#	‡					

See Also clear lacp counters

show lacp-sys-id

Displays the Link Aggregation Control Protocol (LACP) system ID and priority information.

Synopsis show lacp sys-id

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the LACP system ID and priority.

Usage Guidelines The system priority and the system Media Access Control (MAC) address make up the system

identification. The first two bytes are the system priority, and the last six bytes are the globally

administered individual MAC addresses associated with the system.

Examples To display the local system ID:

switch#show lacp sys-id

% System 8000,00-05-le-76-la-a6

show license

Displays license information.

Synopsis show license [switchId switchID | all]

Operands. switchId switchID Executes the command on the remote switch specified by the switch ID.

all Executes the command on all switches in the fabric.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the license information for the local switch or any switch in a VCS

cluster. The command output includes the switch ID, license description, expiration if applicable,

and the feature name. A string of "x" characters is displayed for the license key

Usage Guidelines There are no usage guidelines for this command.

Examples To display license information on a specified switch:

switch# show license switchId 2

SwitchId: 2

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

FCoE Base license Feature name:FCOE_BASE

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

First Ports on Demand license - additional 10 port upgrade license $\,$

Feature name:PORTS_ON_DEMAND_1

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Second Ports on Demand license - additional 10 port upgrade license

Feature name:PORTS_ON_DEMAND_2

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

VCS Fabric license Feature name:VCS

To display license information on all switches in the VCS cluster:

switch# show license all

SwitchId: 2

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

FCoE Base license

Feature name: FCOE_BASE

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

First Ports on Demand license - additional 10 port upgrade license

Feature name:PORTS_ON_DEMAND_1

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Second Ports on Demand license - additional 10 port upgrade license

Feature name:PORTS_ON_DEMAND_2

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

VCS Fabric license Feature name:VCS

SwitchId: 3

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

First Ports on Demand license - additional 10 port upgrade license Feature name:PORTS_ON_DEMAND_1

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Second Ports on Demand license - additional 10 port upgrade license Feature name:PORTS_ON_DEMAND_2

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

VCS Fabric license Feature name:VCS

See Also license add, license remove, show license id

show license id

Displays the switch License ID.

Synopsis show license id [switchId switchID | all]

Operands switchId switchID Executes the command on the remote switch specified by the switch ID.

all Executes the command on all switches in the fabric.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the switch license ID (WWN) for the specified switch. You need the

switch license ID when you add a license.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the license ID for the local switch:

switch# show license id

SwitchId LicenseId

See Also license add, license remove, show license

show IIdp interface

Displays the LLDP status on the specified interface.

Synopsis show lidp interface [tengigabitethernet slot/port]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number. Specifies a valid port number. port

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

> Description Use this command to display the LLDP status on the specified interface.

Usage Guidelines There are no usage guidelines for this command.

> Examples To display all the LLDP interface information for a selected interface:

> > switch#show lldp interface tengigabitethernet 0/0

LLDP information for Te 0/0

State: Enabled

Mode: Receive/Transmit

Advertise Transmitted: 30 seconds Hold time for advertise: 120 seconds Re-init Delay Timer: 2 seconds 1 seconds Tx Delay Timer: DCBX Version : CEE

Auto-Sense : Yes

Transmit TLVs: Chassis ID Port ID IEEE DCBX TTL

> DCBX FCoE App DCBX FCoE Logical Link

Link Prim Brocade Link

DCBX FCoE Priority Bits: 0x8

show IIdp neighbors

Displays LLDP information for all neighboring devices on the specified interface.

Synopsis show lldp neighbors [interface tengigabitethernet slot/port detail]

Operands interface Use this keyword to specify the 10 Gbps Ethernet interface using the

following operand followed by the slot or port number.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

detail Displays all the LLDP neighbor information in detail for the specified

interface.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display LLDP information for all neighboring devices on the specified

interface.

Usage Guidelines If you do not use the interface operand, only the mandatory TLVs are displayed.

Examples To display detailed LLDP neighbor information on a specific interface:

switch#show 11dp neighbors interface tengigabitethernet 0/8 detail

Neighbors for Interface Te 0/8

MANDATORY TLVs

Local Interface: Te 0/8 Remote Interface: Te 0/8 (IF Name)
Dead Interval: 120 secs Remaining Life: 100 secs Tx: 536 Rx: 535

Chassis ID: 0005.1e76.1020 (MAC)

Remote Mac: 0005.1e76.102c

OPTIONAL TLVs

Port Interface Description: Te 0/8

System Name: sw0

System Description: Fibre Channel Switch. System Capabilities: Switching Routing System Capabilities Enabled: Switching

Link Prim: 257

Remote Protocols Advertised: Multiple Spanning Tree Protocol

Remote VLANs Configured: VLAN ID: 1 VLAN Name: default

AutoNego Support: Supported Not Enabled

AutoNego Capability: 0 Operational MAU Type: 0

Link Aggregation Capability: Capable Link Aggregation Status: Disabled

Port Vlan Id: 1

```
Port & Protocol Vlan Flag: Supported Not enabled
Port & Protocol Vlan Id: 0
Link Aggregation Port Id: 0
Max Frame Size: 2500
Management Address: 10.32.152.21 (IPv4)
Interface Numbering: 2
Interface Number: 0x4080100 (67633408)
OID: 0x100f99b4
DCBX TLVs
______
DCBX Version : pre-CEE
DCBX Ctrl OperVersion: 0 MaxVersion: 0 SeqNo: 2 AckNo: 1
DCBX ETS OperVersion: 0 MaxVersion: 0 EN: 1 Will: 0 Err: 0
Pri-Map: 15 15 15 15 15 15 15 15
BWG ID: 00 Percentage: 000
BWG ID: 01 Percentage: 000
BWG ID: 02 Percentage: 000
BWG ID: 03 Percentage: 000
BWG ID: 04 Percentage: 000
BWG ID: 05 Percentage: 000
BWG ID: 06 Percentage: 000
BWG ID: 07 Percentage: 000
DCBX PFC OperVersion: 0 MaxVersion: 0 EN: 1 Will: 0 Err: 0
Admin-Map: 0xf0
FCoE App OperVersion: 0 MaxVersion: 0 EN: 1 Will: 0 Err: 0
User-Pri-Map: 0x00
FCoE LLS OperVersion: 0 MaxVersion: 0 EN: 1 Will: 0 Err: 0
Logic Link Status: Down
LAN LLS OperVersion: 0 MaxVersion: 0 EN: 1 Will: 0 Err: 0
Logic Link Status: Up
switch#
```

show IIdp statistics

Displays the LLDP statistics on all interfaces or a specified interface.

Synopsis show lldp statistics [interface tengigabitethernet slot/port]

Operands interface Use this keyword to specify the 10 Gbps Ethernet interface using the

following operand followed by the slot or port number:

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display LLDP statistics on all interfaces or a specified interface.

Usage Guidelines If you do not specify the interface tengigabitethernet operands, this command displays the LLDP

statistics for all interfaces.

Examples To display LLDP statistics on the specified interface:

 $\verb|switch#show| 1 | \texttt{ldp} | \texttt{statistics} | \texttt{interface}| \texttt{tengigabitethernet}| \texttt{0/8}|$

LLDP Interface statistics for Te 0/8

Frames transmitted: 555
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Recieved: 554
TLVs discarded: 0
TLVs unrecognized: 0

show logging

Displays the internal RASlog buffer of the switch.

Synopsis show logging

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the RASlog messages stored in the internal buffer.

Usage Guidelines The RASlog messages contain the module name, error code, and message details.

Examples To display the RASlog messages stored in the internal buffer:

switch#show logging

Fabos OS Version: v6.1.2

Number of Messages: 1024

2009/02/03-00:19:43: %NSM-4-1001: Interface TenGigabitEthernet 0/4 is

online.

2009/02/03-00:20:14: %NSM-4-1002: Interface TenGigabitEthernet 0/4 is

protocol down.

2009/02/03-00:20:14: %NSM-4-1001: Interface TenGigabitEthernet 0/4 is

online.

2009/02/03-00:21:10: %NSM-4-1003: Interface Port-channel 10 is link down

show logging raslog

Displays the saved RASlog system messages.

Synopsis show logging raslog [switchid switchID]

Operands switchid switchID Executes the command on a switch specified by its switch ID.

Defaults Displays the messages for the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the saved RASlog messages. For each message, this command

displays the following information:

Timestamp for the message.

Message ID Message identifier.

External sequence number

Sequence number for the message.

Severity Severity of the message. Valid values include INFO, WARNING, ERROR, and

CRITICAL.

Chassis name Chassis name for the generator of this message.

Message body.

Usage Guidelines The messages are dumped to the console without page breaks.

Examples To display the saved RASlog messages on the local switch:

switch# show logging raslog

NOS: v2.0.0

2000/03/10-14:01:33, [NSM-2006], 12592,, INFO, AMPP_SK_112, Port-profile aal removed successfully on TenGigabitEthernet 2/0/17

2000/03/10-14:02:24, [NSM-2004], 12593,, INFO, AMPP_SK_112, Port-profile aal application succeeded on TenGigabitEthernet 2/0/17

2000/03/10-14:02:31, [NSM-2004], 12594,, INFO, AMPP_SK_112, Port-profile aal application succeeded on TenGigabitEthernet 2/0/14

2000/03/10-14:07:03, [NSM-2006], 12595,, INFO, AMPP_SK_112, Port-profile aal removed successfully on TenGigabitEthernet 2/0/14

2000/03/10-14:09:05, [HIL-1404], 12596,, WARNING, Brocade8000, 1 fan FRUs missing. Install fan FRUs immediately.

[output truncated]

See Also clear logging raslog, logging switchid raslog console, show running-config logging

show mac access-group

Displays the current MAC ACL mapping to interfaces.

Synopsis show mac access-group [interface port-channel number | tengigabitethernet slot/port | vlan

vlan_id]

Operands interface Specifies the interface for which to display the MAC ACL mapping.

port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

3583.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the current MAC ACL mapping to interfaces.

Usage Guidelines If you do not specify an interface, this command shows the mapping of MAC ACL to all interfaces.

Examples To display the current MAC ACL mapping for 10 Gbps Ethernet interface 0/1:

```
switch#show mac access-group interface tengigabitethernet 0/1
Interface Te 0/1
    Inbound access-list is std_acl
```

To display the current MAC ACL mapping for interface VLAN 100:

```
switch#show mac access-group interface vlan 100
Interface Vl 100
    Inbound access-list is ext_acl
```

To display the current MAC ACL mapping for 10 Gbps Ethernet interface 0/7 where there is no ACL applied:

```
switch#show mac access-group interface tengigabitethernet 0/7
Interface Te 0/7
    Inbound access-list is not set
```

See Also show running-config, show statistics access-list mac

show mac-address-table

Displays a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries for a specific interface or VLAN.

Synopsis show mac-address-table [address mac-addr | aging-time | count | dynamic | interface

[tengigabitethernet slot/port | port-channel number] | linecard interface tengigabitethernet

slot/port | static | vlan vlan_id | port-profile name]

Operands address mac-address

Specifies a 48-bit MAC address. The valid format is H.H.H (available in

Privileged EXEC mode only).

aging-time Displays the aging time.

count Displays the count of forwarding entries.

dynamic Displays the dynamic MAC addresses.

interface Displays the forwarding information of an interface.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

linecard interface tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

static Displays the static MAC addresses.

vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

3583.

port-profile name Specifies a valid AMPP port-profile name.

Defaults No static addresses are configured.

Command Modes Privileged EXEC mode

Description Use this command to display a specific static or dynamic MAC address entry or all entries for a

specific interface, a specific VLAN, a specific linecard, or for all interfaces and all VLANs.

Usage Guidelines There are no usage guidelines for this command.

Examples To display a specific MAC address in the table:

switch#show mac-address-table address 0011.2222.3333
VlanId Mac-address Type State Ports

vianid Mac-address Type State Ports
100 0011.2222.3333 Static Inactive Te 0/1

Total MAC addresses : 1

To display the aging time for a specific MAC address table:

```
switch#show mac-address-table aging-time
MAC Aging-time : 300 seconds
```

To display a dynamic MAC address table:

switch#show mac-address-table dynamic

VlanId	Mac-address	Type	State	Ports
100	0011.2222.5555	Dynamic	Inactive	Te 0/1
100	0011.2222.6666	Dynamic	Inactive	Te 0/1
Total N	MAC addresses :	2		

show media

Displays the SFP information for all the interfaces present on a switch.

Synopsis show media

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display a summary of all SFP information for the switch. The output will be

several pages long.

Usage Guidelines There are no usage guidelines for this command.

Examples To display all SFP information:

```
switch#show media interface tengigabitethernet 0/1
```

```
Interface TenGigabitEthernet 0/1
  Identifier 3
                      SFP
  Connector
                7
                      LC
 Transceiver 00000000000010 10_GB/s
 Name
                id
 Encoding 6
Baud Rate 103 (units 100 megabaud)
Length 9u 0 (units km)
Length 9u 0 (units 100 meters)
Length 50u 8 (units 10 meters)
 Encoding
 Length 62.5u 3 (units 10 meters)
 Length Cu 0 (units 1 meter)
 Vendor Name BROCADE
 Vendor OUI 42:52:4f
 Vendor PN
               57-0000075-01
 Vendor Rev A
 Wavelength 850 \text{ (units nm)}
 Options 001a Loss_of_Sig,Tx_Fault,Tx_Disable
 BR Max
                 0
 BR Min
               0
 Serial No AAA108454100431
Date Code 081108
 Temperature 44 Centigrade
  Voltage 3246.8 (Volts)
                 0.002 (mAmps)
  Current
  TX Power
                0.1 (uWatts)
  RX Power
                 0.1 (uWatts)
(output truncated)
```

See Also show media interface, show media linecard

show media interface

Displays the SFP information for a specific interface.

Synopsis show media interface [tengigabitethernet slot/port]

Operands tengigabitethernet

Specifies a valid external 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display a summary of the SFP information for the specified interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To display SFP information for 10 Gbps Ethernet interface:

switch#show media interface tengigabitethernet 0/1

```
Interface TenGigabitEthernet 0/1
  Identifier 3
                       SFP
                 7
  Connector
                       LC
 Transceiver 000000000000010 10_GB/s
 Name
                 id
               6
 Encoding 6
Baud Rate 103 (units 100 megabaud)
Length 9u 0 (units km)
Length 9u 0 (units 100 meters)
Length 50u 8 (units 10 meters)
  Encoding
  Length 62.5u 3 (units 10 meters)
 Length Cu 0 (units 1 meter)
  Vendor Name BROCADE
  Vendor OUI 42:52:4f
  Vendor PN
                 57-0000075-01
  Vendor Rev
              A
  Wavelength 850 (units nm)
  Options
                 001a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max
 serial No AAA108454100431
Date Code 081100
  BR Min
                 0
  Temperature
                 44 Centigrade
  Voltage
                 3246.8 (Volts)
  Current
                 0.002 (mAmps)
                 0.1 (uWatts)
  TX Power
  RX Power
                 0.1 (uWatts)
```

See Also show media, show media linecard

show media linecard

Displays the SFP information for all the interfaces of a specific line card.

Synopsis show media linecard number

Operands *number* Linecard number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display a summary of the SFP information for a specific line card. The output

contains information for each interface on the line card, and is several pages long.

Usage Guidelines There are no usage guidelines for this command.

Examples To show the SFP information for line card number 0:

```
switch#show media linecard 0
Interface TenGigabitEthernet 0/1
  Identifier 3
                      SFP
  Connector
                7
                      LC
  Transceiver 000000000000010 10_GB/s
 Name
                id
 Encoding 6
Baud Rate 103 (units 100 megabaud)
Length 9u 0 (units km)
Length 9u 0 (units 100 meters)
Length 50u 8 (units 10 meters)
  Encoding
 Length 62.5u 3 (units 10 meters)
 Length Cu 0 (units 1 meter)
 Vendor Name BROCADE
 Vendor OUI 42:52:4f
               57-0000075-01
 Vendor PN
 Vendor Rev A
 Wavelength 850 (units nm)
  Options 001a Loss_of_Sig,Tx_Fault,Tx_Disable
 BR Max
                0
 BR Min
               0
 Serial No AAA108454100431
Date Code 081108
 Temperature 44 Centigrade
  Voltage 3246.8 (Volts)
                0.002 (mAmps)
  Current
  TX Power
               0.1 (uWatts)
  RX Power
                 0.1 (uWatts)
(output truncated)
```

See Also show media interface, show media

show monitor

Displays the monitoring information for all Port Mirroring sessions.

Synopsis show monitor

show monitor session session_number

Operands session_number

Specifies a session identification number. The range of valid values is from

0 to 65535.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display monitoring information for all Port Mirroring sessions, or for a single

session.

Usage Guidelines There are no usage guidelines for this command.

Examples To display monitoring information for all Port Mirroring sessions:

switch#show monitor

See Also monitor session

show name-server

Displays local name server (NS) information about devices connected to a switch.

Synopsis show name-server [brief domainId] [detail]

Operands brief Displays brief name server entries.

domainId Specifies the domain identifier on which the brief name server entries are

displayed.

detail Displays detailed name server entries.

Description Use this command to display local name server (NS) information about devices connected to a

switch.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines If no information is available for the switch, the command displays the message: "There is no entry

in the Local Name Server."

Examples The first example shows the brief nameserver entries for a specified domain ID and the second

example displays the detailed nameserver entries. In the second example, the VCS switch is

connected to an FCoE initiator port.

switch# show name-server brief domainID 9
 010000 020100 030200 010300 020400 030500 010600 020700 030800

switch# show name-server detail

PID: 012100

Port Name: 10:00:00:05:1E:ED:95:38
Node Name: 20:00:00:05:1E:ED:95:38

SCR: 3 FC4s: FCP

PortSymb: [27] "Brocade-1020|2.3.0.0|localhost.localdomain|Red Hat

Enterprise Linux Server release 5.5"

NodeSymb: NULL

Fabric Port Name: 20:21:00:05:1E:CD:79:7A
Permanent Port Name: 10:00:00:05:1E:ED:95:38

Device type: Physical Initiator

Interface: Fcoe 1/1/9
Physical Interface: Te 1/0/9

Share Area: No Redirect: No

show ntp status

Displays the current active NTP server IP address or LOCL (for local switch time when no NTP

servers were configured or no reachable NTP servers are available).

Synopsis show ntp status [switchid switch-id | all]

Operands switchid

switchid | all | Specifies the switch ID on which the NTP server status displays. For this

release, specifying all returns only local information.

Description Use this command to display the active NTP server.

Defaults The local clock is used unless the switch ID or all is specified.

Command Modes Privileged EXEC mode

Usage Guidelines The request is for the local switch, unless the switch ID is specified.

Examples switch# show ntp status all

switchid 1: active ntp server is 10.31.2.81

switch# show ntp status switchid 1

switchid 1: active ntp server is 10.31.2.80

See Also diag post

show port-channel

Displays the Link Aggregation Group (LAG) information for a port-channel.

Synopsis show port-channel [channel-group-number | detail | load-balance | summary]

Operands channel-group-number

Specifies a LAG port channel-group number to display. The range of valid

values is from 1 through 63.

detail Displays detailed LAG information for a port-channel.

load-balance Displays the load-balance or frame-distribution scheme among ports in the

port-channel.

summary Displays the summary information per channel-group.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Displays the LAGs present on the system with details about the LACP counters on their member

links. LAG interfaces are called port-channels.

Usage Guidelines If you do not specify a port-channel, all port-channels are displayed.

Examples To display information for port-channel 10:

```
switch#show port-channel 10
```

% Aggregator Po 10 0 Admin Key: 0010 - Oper Key 0010 Partner System ID:
0x0000,00-00-00-00-00-00 Partner Oper
Key 0000

% Link: Te 0/1 (67174401) sync: 0
% Link: Te 0/2 (67239938) sync: 0

show port-profile

Displays the AMPP port-profile configuration information.

Synopsis show port-profile [name profile-name [vlan | qos | security]]

Operands name profile-name Specifies a valid AMPP por-prtofile name.

vlan Displays the AMPP profile for VLAN.qos Displays the AMPP profile for QoS.security Displays the AMPP profile for security.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the port-profile configuration for all AMPP profiles.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also show running-config, show port-profile interface, show port-profile status

show port-profile interface

Displays AMPP port-profile information for interfaces.

Synopsis show port-profile interface [all | tengigabitethernet slot/port]

Operands all Displays the port-profile information for all interfaces.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no default configurations for this command

Command Modes Privileged EXEC mode

Description Use this command to display AMPP port-profile information for either all interfaces, or for specific

interfaces.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also show running-config, show port-profile, show port-profile status

show port-profile status

Displays the status of AMPP profiles.

Synopsis show port-profile status [activated | associated | applied] | [name profile-name status [activated

| associated | applied]]

Operands activated Show all port-profiles with the activated status.

associated Show all port-profiles with the associated status.

applied Show all port-profiles with the applied status.

name profile-name status

Specifies the profile to display.

activated Show all port-profiles with the activated status for the given profile.

Show all port-profiles with the associated status for the given profile.

Show all port-profiles with the applied status for the given profile.

Defaults There are no default configurations for this command

Command Modes Privileged EXEC mode

Description Use this command to display the port-profile status.

Use the show port-profile version of this command to display the status of all AMPP profiles.

Examples None

See Also show running-config, show port-profile, show port-profile interface

show process

Displays system process information.

Synopsis show process { info | memory | cpu } [switchid { switchID | all }]

Operands cpu Displays processes by percent of CPU usage.

info Displays processes hierarchically.

memory Displays processes by memory usage (in KB).

switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display system processes by memory usage, by CPU usage, or in hierarchical

order.

Usage Guidelines Pagination is not supported with the **all** option.

Examples To display system processes hierarchically:

```
switch#show process info
```

```
PID COMMAND
    1 init [3]
    2 [ksoftirqd/0]
    3 [events/0]
    4 [khelper]
   5 [kthread]
   36 \_ [kblockd/0]
   69 \_ [pdflush]
   70 \_ [pdflush]
   72 \_ [aio/0]
 1038 \_ [eth0/0]
 1054 \setminus [eth1/0]
 1865 \_ [kwt_nb_thread]
   71 [kswapd0]
  801 [kjournald]
 819 /sbin/wdtd -p 30 -n 5
 880 [kjournald]
 1069 /sbin/portmap
 1086 /usr/sbin/inetd
 1106 /usr/sbin/syslogd -m 0
 1107 /usr/sbin/klogd -x
[output truncated]
```

To display system processes by CPU usage:

```
switch# show process cpu
%CPU CPU NI S
                  TIME COMMAND
0.0 - -5 S 00:00:00 [khelper]
0.0 - -5 S 00:00:00 [kthread]
0.0 - -5 S 00:00:00 [kblockd/0]
0.0 - 0 S 00:00:00 [pdflush]
0.0 - -5 S 00:00:00 [aio/0]
0.0 - 0 S 00:00:00 [kswapd0]
     - - S 00:00:00 /sbin/wdtd -p 30 -n 5
0.0
0.0 - -5 S 00:00:00 [eth0/0]
     - -5 S 00:00:00 [eth1/0]
- -5 S 00:00:00 [kwt_nb_thread]
0.0
0.0
0.0 - 0 S 00:00:00 [kmtracer]
0.0 - 0 S 00:00:00 [ISCK_TH]
0.0 - 0 S 00:00:00 [RTEK_TH]
0.0 - 0 S 00:00:00 [dpod_daemon]
0.0 - 0 S 00:00:00 /sbin/getty -h ttyS0 console
[output truncated]
```

To display system processes by memory usage:

switch#	show	process	memo	ory
PID	SZ	VSZ	RSS	CMD
AMPP_SK_	_112#	1	232	1700 584 init [3]
2	0	0	0	[ksoftirqd/0]
3	0	0	0	[events/0]
4	0	0	0	[khelper]
5	0	0	0	[kthread]
36	0	0	0	[kblockd/0]
69	0	0	0	[pdflush]
70	0	0	0	[pdflush]
72	0	0	0	[aio/0]
71	0	0	0	[kswapd0]
801	0	0	0	[kjournald]
819	232	1680	404	/sbin/wdtd -p 30 -n 5
880	0	0	0	[kjournald]
1038	0	0	0	[eth0/0]
1054	0	0	0	[eth1/0]
1069	236	1692	420	/sbin/portmap
1086	416	2120	640	/usr/sbin/inetd
[output	trund	cated]		

show processes cpu

Displays information about the active processes in the switch and their corresponding CPU utilization statistics.

Synopsis show processes cpu [summary]

Operands summary Shows a summary of CPU usage by all processes.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display information about the active processes in the switch and their

corresponding CPU utilization statistics.

Usage Guidelines There are no usage guidelines for this command.

Examples To show the information for all processes:

```
switch#show processes cpu summary
CPU Utilization current: 0.90%; One minute: 0.00%; Five minutes: 0.00%;
Fifteen minutes: 0.00%
```

To show CPU usage information by individual processes:

```
\verb|switch| \# \textbf{show processes cpu}|
```

CPU Utilization current: 0.90%; One minute: 0.00%; Five minutes: 0.00%; Fifteen minutes: 0.00%

PID	Process	CPU%	State	Started			
1	init	0.00	S	14:18:35	Feb	19,	2009
2	ksoftirqd/0	0.00	S	14:18:35	Feb	19,	2009
3	events/0	0.00	S	14:18:35	Feb	19,	2009
4	khelper	0.00	S	14:18:35	Feb	19,	2009
5	kthread	0.00	S	14:18:35	Feb	19,	2009
40	kblockd/0	0.00	S	14:18:35	Feb	19,	2009
73	pdflush	0.00	S	14:18:35	Feb	19,	2009

show processes memory

Displays the memory usage information based on processes running in the system.

Synopsis show processes memory [summary]

Operands summary Shows a summary of memory usage by all processes.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to view memory usage information based on processes running in the system.

Usage Guidelines There are no usage guidelines for this command.

Examples To show a summary of memory usage by all processes:

```
switch#show processes memory summary
```

%Memory Used: 39.463%; TotalMemory: 1028020 KB; Total Used: 405688 KB; Total Free: 622332 KB

To show memory usage information by individual processes:

switch#show processes memory

%Memory Used: 39.463%; TotalMemory: 1028020 KB; Total Used: 405688 KB; Total

Free: 622332 KB

PID	Process	MEM%	Mem Used(bytes)	Heap Total	Heap Used
1	init	0.00	1736704	-	-
2	ksoftirqd/0	0.00	0	-	-
3	events/0	0.00	0	-	-
4	khelper	0.00	0	-	-
5	kthread	0.00	0	_	-

show protect-mode status

Displays the current status of protect mode.

Synopsis show protect-mode status

Operands None

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to display the current status of protect mode.

Usage Guidelines There are no usage guidelines for this command.

Examples None

show gos flowcontrol interface

Displays all of the configured flow control information for an interface.

Synopsis show gos flowcontrol interface [tengigabitethernet slot/port | linecard slot | portset chip | all]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

linecard portset Reports the QoS flow control statistics for all 10 Gbps Ethernet interfaces

within an ASIC.

slot Specifies the ASIC linecard slot number within the chassis.

chip Specifies the ASIC number within the linecard.

all Reports QoS flow control statistics for all interfaces within the system.

Command Modes Privileged EXEC mode

Description Use this command to display all of the configured flow control information for a specific interface.

Usage Guidelines

Use this command to display the runtime state retrieved from the dataplane reflecting the operation of 802.3x pause or Priority Flow Control (PFC) on an interface. The administrative state for pause generation and reception or processing is presented for the interface (802.3x mode) or for each CoS (PFC mode). TX_Pause frame generation statistics are always presented for the interface. The RX_Pause BitTimes is presented for the interface (802.3x mode) or for each CoS (PFC mode). When PFC is deployed under the CEE Provisioning model, then the command reports whether the Data Center Bridging eXchange protocol (DCBX) has overridden the user configuration, for example when the DCBX detects a mis-configuration between CEE peers, it disables PFC operationally.

Examples

To display all of the configured flow control information for a 10 Gbps Ethernet interface:

switch#show qos flowcontrol interface tengigabitethernet 0/1

Interface TenGigabitEthernet 0/1
 Mode PFC
 DCBX enabled for PFC negotiation
 TX 0 frames

	TX	TX	RX	RX	Output Paused
CoS	${\tt Admin}$	Oper	${\tt Admin}$	Oper	512 BitTimes
0	Off	Off	Off	Off	0
1	Off	Off	Off	Off	0
2	On	Off	On	Off	0
3	Off	Off	Off	Off	0
4	Off	Off	Off	Off	0
5	Off	Off	Off	Off	0
6	Off	Off	Off	Off	0
7	Off	Off	Off	Off	0

See Also

show qos interface, show cee maps

show gos interface

Displays a summary of all QoS configurations applied on an interface.

Synopsis show qos interface [tengigabitethernet slot/port | port-channel number | all]

Operands tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number. Use this keyword to specify any of the following

interfaces:

port-channel number

Specifies the port-channel of the interface. The range of valid values is from

1 through 63.

all Reports QoS configurations for all interfaces within the system.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display a summary of all QoS configuration applied on an interface, including

QoS Provisioning mode, CEE map, Layer 2 priority, Traffic Class mapping, congestion control, and

the scheduler policy.

Usage Guidelines If no interface is specified, QoS information about all interfaces is displayed.

Examples To display all of the configured QoS information for a 10 Gbps Ethernet interface:

```
switch#show qos interface tengigabitethernet 0/1
Interface TenGigabitEthernet 0/1
 Provisioning mode cee
 CEE Map demo
 Default CoS 0
 Interface trust cos
 CoS-to-CoS Mutation map 'default'
                In-CoS: 0 1 2 3 4 5 6 7
    Out-CoS/TrafficClass: 0/4 1/4 2/6 3/4 4/4 5/4 6/4 7/4
 Tail Drop Threshold 1081344 bytes
 Per-CoS Tail Drop Threshold (bytes)
         CoS:
                0 1 2
    Threshold: 129761 129761 129761 129761 129761 129761 129761 129761
 Flow control mode PFC
    CoS2 TX on, RX on
 Multicast Packet Expansion Rate Limit 3000000 pkt/s, max burst 4096 pkts
 Multicast Packet Expansion Tail Drop Threshold (packets)
TrafficClass: 0 1 2 3 4 5 6
             64 64
                     64 64 64 64 64
Threshold:
                                             64
 Traffic Class Scheduler configured for 0 Strict Priority queues
    TrafficClass: 0 1 2 3 4 5 6 7
      DWRRWeight: 0 0 0 0 60 0 40
```

Multicast	Packet	Expar	nsion	Traf	Eic Cl	lass :	Sched	uler
TrafficClass	s: 0	1	2	3	4	5	6	7
DWRRWeight:	25	25	25	25	25	25	25	25

See Also cee-map (FCoE), priority-table

show qos maps

Displays information on the defined QoS maps.

Synopsis show gos maps [cos-mutation [name] | cos-traffic-class [name]]

Operands cos-mutation name

Specifies to report on only the named CoS-to-CoS mutation QoS map.

cos-traffic-class name

Specifies to report on only the named CoS-to-Traffic Class QoS map.

Defaults The default behavior without any specified operands is to report on all defined QoS maps.

Command Modes Privileged EXEC mode

Description Use this command to display information on the QoS defined maps. For each QoS map, the

configuration state is displayed with a list of all interfaces bound to the QoS map.

Usage Guidelines There are no usage guidelines for this command.

Examples To display information on the defined QoS maps:

```
switch#show qos maps
```

```
CoS-to-CoS Mutation map 'test'
    In-CoS: 0 1 2 3 4 5 6 7
    Out-CoS: 0 1 2 3 5 4 6 7
    Enabled on the following interfaces:
    Te 0/5

CoS-to-Traffic Class map 'test'
    Out-CoS: 0 1 2 3 4 5 6 7
```

TrafficClass: 0 1 2 3 5 4 6 7
Enabled on the following interfaces:
Te 0/5

See Also qos map cos-traffic-class, show qos interface

show qos queue interface

Displays the runtime state retrieved from the interface reflecting the number of packets and bytes sent and received for each priority.

Synopsis show gos queue interface [tengigabitethernet slot/port | all]

Operands tengigabitethernet Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.port Specifies a valid port number.

all Reports QoS statistics for all 10 Gbps interfaces within the system.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the runtime state retrieved from the interface reflecting the number

of packets and bytes sent and received for each priority.

Usage Guidelines For a stand-alone switch, all ASICs are considered as slot number zero (0).

Examples To display the queueing information for a 10 Gbps Ethernet interface:

switch#show qos queue interface tengigabitethernet 0/2

 ${\tt Interface\ TenGigabitEthernet\ 0/2}$

RX Packets	RX		TX	TX
Daakota				===
Packets	Bytes	TC	Packets	Bytes
680458	87098624	0	0	0
0	0	1	32318	0
0	0	2	0	0
0	0	3	0	0
0	0	4	0	0
0	0	5	0	0
0	0	6	0	0
0	0	7	0	0
_	680458 0 0 0 0 0		680458 87098624 0 0 0 1 0 0 2 0 0 3 0 0 4 0 0 5	680458 87098624 0 0 0 0 1 32318 0 0 2 0 0 0 3 0 0 0 4 0 0 0 5 0

See Also qos map cos-mutation, cee-map (Configuration)

show gos rcv-queue interface

Displays a summary the runtime ingress queue state information.

Synopsis show qos rcv-queue interface [tengigabitethernet slot/port | all]

Operands tengigabitethernet Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

all Reports QoS configurations for all 10 Gbps Ethernet interfaces within the

system.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display a summary the runtime ingress queue state information applied to a

Layer 2 interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the runtime ingress queue state information retrieved from the dataplane for a 10 Gbps

Ethernet interface:

 $\verb|switch| \# show qos rcv-queue interface tengigabitethernet 0/2|\\$

Interface TenGigabitEthernet 0/2

In-use 404019 bytes, Total buffer 1081344 bytes

0 packets dropped

	In-use	Max
CoS	Bytes	Bytes
0	0	1081344
1	0	1081344
2	404019	1081344
3	0	1081344
4	0	1081344
5	0	1081344
6	0	1081344
7	0	1081344

See Also show gos rcv-queue multicast

show gos rcv-queue multicast

Displays the runtime state retrieved from the dataplane reflecting any multicast packet expansion packet drops resulting from a queue crossing the maximum queue depth.

Synopsis show gos rcv-queue multicast [tengigabitethernet s/ot/port | all]

Operands tengigabitethernet Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

all Reports QoS multicast packet expansion receive queueing statistics for all

ASICs within the system.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the runtime state information retrieved from the interface reflecting

any multicast packet expansion packet drops resulting from a queue crossing the maximum queue

depth.

Usage Guidelines For a stand-alone switch, all ASICs are considered as slot number zero (0).

Examples To display the queueing information:

switch#show qos rcv-queue multicast tengigabitethernet 0/2

Dropped Counts

Linecard/Portset TC 0 TC 1 TC 2 TC 3

See Also show gos rcv-queue interface

show rmon

Displays the current RMON status on the switch.

Synopsis show rmon [alarms [number] [brief] | events [number] [brief] | logs [event_number] | statistics

[number] [brief]]

Operands alarms Specifies to display the RMON alarm table.

number Specifies the alarm index identification number. The range of valid values is

from 1 through 65535.

brief Specifies to display a brief summary of the output.

events Specifies to display the RMON events table.

number Specifies the event index identification number. The range of valid values is

from 1 through 65535.

brief Specifies to display a brief summary of the output.

logs Specifies to display the RMON log table.

event_number Specifies the event log index identification number. The range of valid values

is from 1 through 65535.

statistics Specifies to display the statistics identification number.

number Specifies the statistics identification number. The range of valid values is

from 1 through 65535.

brief Specifies a brief summary of the output.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the status of the current RMON on the switch.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the RMON statistics:

```
switch#show rmon statistics
```

```
rmon collection index 4

Interface index is Id: 67108864 , Name : TenGigabitEthernet 0/0
Receive Statistics:

218903 packets, 14015626 bytes, 0 packs dropped
Multicasts: 218884, Broadcasts: 18

Under-size : 0, Jabbers: 0, CRC: 0
Fragments: 0, Collisions: 0
64 byte pkts: 218722, 65-127 byte pkts: 174
128-255 byte pkts: 0, 256-511 byte pkts: 6
512-1023 byte pkts: 0, 1024-1518 byte pkts: 0
Over 1518-byte pkts(Oversize - Jumbo): 0

Owner: RMON_SNMP
```

Status: ok(1)

To display the RMON events:

See Also rmon alarm, rmon event

show rmon history

Displays information gathered by **rmon event** and **rmon alarm** commands.

Synopsis show rmon history [statistics | history_index]

Operands statistics Displays a more detailed synopsis.

history_index Specifies the rmon history identification number. The range of valid values is

from 1 through 65535.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Displays a synopsis of the statistics collected by the **rmon event** and **rmon alarm** commands.

Usage Guidelines Use the statistics option to display the detailed history.

Examples To display the RMON history:

switch#show rmon history
RMON history control entry 1

interface: ifIndex.1745682445 TengigabitEthernet 0/13

buckets requested: 20
buckets granted: 20
sampling interval: 10

Owner: jsmith

See Also rmon alarm, rmon event

show running-config

Displays the contents of the running configuration.

Synopsis show running-config

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running configuration. The running configuration is the

configuration that is currently active on the local switch but not saved persistently.

Usage Guidelines This command is supported only on the local switch.

Examples To display the running configuration:

```
switch# show running-config
logging switchid 2
raslog console INFO
logging syslog ipaddress [ ]
switch-attributes 2
chassis-name chassis
host-name sw
support switchid 2
ffdc
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr
snmp-server community "Secret COde"
!
snmp-server community common
snmp-server community private
snmp-server community public
[output truncated]
```

See Also copy, copy running-config startup-config, delete, dir, chassis disable, show file, show support, vcs

show running-config aaa

Displays user configuration attributes for authentication, authorization, and accounting (AAA) from

the configuration database.

Synopsis show running-config aaa

Operands None

Description Use this command to show configuration attributes for an AAA server.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples Example of displaying the authentication mode:

switch# show running-config aaa

aaa authentication login tacacs+ local

See Also aaa authentication

show running-config banner

Displays the configured banner.

Synopsis show running-config banner

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the banner configured for the switch.

Usage Guidelines There are no usage guidelines for this command.

Examples To set and display a banner:

switch# show running-config banner

% No entries found.
switch#configure

switch(config)#banner login "Please don't disturb the setup on this switch."

 $\verb|switch(config)| \# \textbf{exit}|$

Login as: admin Password: ****

Please don't disturb the setup on this switch.

Welcome to the Brocade Network Operating System Software adminconnected from 10.120.34.144 using ssh on sw0

See Also vcs

show running-config dpod

Displays license information.

Synopsis show running-config dpod [slot/port]

Operands slot Specifies the slot number.

port Specifies the port number.

Operands None

Defaults Displays all port reservations on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display port reservations for a specified port or for all ports on the local

switch.

Usage Guidelines This command is not supported in VCS mode.

Examples To display port reservations for all ports on the local switch:

```
switch# show running-config dpod
dpod 0/1
  reserve
!
dpod 0/2
!
dpod 0/3
!
dpod 0/4
!
dpod 0/5
  reserve
!
dpod 0/24
  reserve
!
```

To display port reservations for port 11:

```
switch# show running-config dpod 0/11
dpod 0/11
  reserve
!
```

See Also dpod, show dpod

show running-config fabric route mcast

Displays fabric route multicast configuration information.

Synopsis show running-config fabric route mcast

Operands None

Description Use this command to display fabric route multicast configuration information.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Usage Guidelines The configuration currently effective on the switch is referred to as the running configuration. Any

configuration change you make while the switch is online is made to the running configuration.

Examples The following example displays fabric route multicast configuration information:

switch# show running-config fabric route mcast

fabric route mcast rbridgeId 2

See Also fabric route multicast, show fabric route multicast

show running-config fcoe

Displays the running configuration for FCoE.

Synopsis show running-config fcoe [fabric-map default | map default]

Operands fabric-map default Displays the contents of the fabric map.

map default Displays the list of available maps.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description This command displays the currently running configuration for FCoE.

Usage Guidelines There are no usage guidelines for this command.

Examples switch#show running-config fcoe fabric-map default

fcoe

fabric-map default
 vlan-id 1002
 virtual-fabric 1
 priority 3
 fcmap 0E:FC:00

advertisement interval 8000

keep-alive timeout

switch# show running-config fcoe map default

fcoe

map default

fabric-map default
cee-map default

See Also None

show running-config igmp

Displays the IGMP configuration.

Synopsis show running-config igmp

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description This command displays the IGMP contents of the currently running configuration. Note that this

information may differ from the contents of the actual running-config file.

Usage Guidelines There are no usage guidelines for this command.

Examples None

See Also None

show running-config interface management

Displays the management interface configuration parameters.

Synopsis show running-config interface management [switchID/0]

Operands switchID/O Specifies the switch ID for the management interface.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the management interface configuration parameters. These

parameters are set by the interface management command.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the management interface configuration parameters for switch 2:

```
switch# show running-config management 2/0
interface Management 2/0
no ip address dhcp
ip address 10.20.49.112/20
ip gateway-address 10.20.48.1
ipv6 address ""
no ipv6 address autoconfig
```

See Also interface management, show interface management

show running-config logging

Displays the severity level configured for the RASlog console.

Synopsis show running-config logging [switchid switchID raslog console]

Operands switchid switchID Executes the command on a switch specified by its switch ID.

Defaults Displays the information for the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configured severity levels for the RASlog console. Valid values

consist of one of the following: INFO, WARNING, ERROR, or CRITICAL.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the severity level configured for the RASlog console:

```
switch# show running-config logging
logging switchid 2
raslog console INFO
!
```

See Also clear logging raslog, logging switchid raslog console, show logging raslog

show running-config logging syslog-server

Displays the syslog server IP addresses.

Synopsis show running-config logging syslog-server

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the servers that are running the syslogd daemon and to which

system messages are sent. Servers are specified in the configuration database by IP address.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the syslog daemon IP addresses configured on a switch:

switch# show running-config logging syslog-server

logging syslog-server 192.168.163.233 logging syslog-server 192.168.163.234

See Also logging syslog-server

show running-config password-attributes

Displays global password attributes.

Synopsis show running-config password-attributes

Operands None

Description Use this command to display global password attributes.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines The attributes will not be displayed when they hold default values.

Examples switch# show running-config password-attributes

password-attributes max-retry 4

password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1

See Also password-attributes, service password-encryption

show running-config radius-server

Displays user configuration for the RADIUS server from the configuration database.

Synopsis show running-config radius-server

Operands None

Description Use this command to display RADIUS server configuration parameters.

Defaults Theere are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples switch# show running-config radius-server ?

Possible completions:

10.xx.xx.xx IP Address or Hostname of this RADIUS server 10.xx.xx.x IP Address or Hostname of this RADIUS server

switch# show running-config radius-server host 10.xx.xx.x

radius-server host 10.xx.xx.x key new#vcs*secret

retransmit 100 timeout 3

See Also radius-server, show running-config tacacs-server, tacacs-server

show running-config role

Displays the configuration for the roles assigned to a user.

Synopsis show running-config role [name role_name]

Operands name The name of the role assigned to the user.

role_name Specifies the name of the role assigned to the user.

Description Use this command to display roles that have been created and the rules with which they are

associated.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples The following example shows the display of a user's assigned roles.

switch# show running-config role

role name VLANAdmin desc "Manages security CLIs" role name NetworkAdmin desc "Manages Network CLIs" role name ClusterAdmin desc "Manages Cluster CLIs"

See Also diag post, rule, show running-config rule

show running-config rule

Displays the configuration for the rules associated with a user's role.

Synopsis show running-config rule [index]

Operands index A numeric identifier of the rule. The valid range is from 1 through 1024. This

field is mandatory.

Description Use this command to display rules that have been defined and associated with a particular role.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples The following example displays rules that are assigned to a user's assigned role.

show running-config rule 30

rule 30

action accept operation read-write role NetworkSecurityAdmin command role

rule 31

action accept operation read-write role NetworkSecurityAdmin

command rule

rule 32

action accept operation read-write role ${\tt NetworkSecurityAdmin}$

command username

rule 33

action accept operation read-write role NetworkSecurityAdmin

 ${\tt command} \ {\tt aaa}$

rule 34

action accept operation read-write role NetworkSecurityAdmin

command radius-server

rule 35

action accept operation read-write role NetworkSecurityAdmin

command configure

rule 40

action accept operation read-write role FCOEAdmin

command "interface fcoe"

See Also diag post, rule, show running-config role

show running-config snmp-server

Shows the user configuration for SNMP.

Synopsis show running-config snmp-server

Operands None

Description Use this command to display the current SNMP configurations of host, community, contact, and

location.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples switch# show running-config snmp-server

snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret COde" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server host 10.32.147.6 common version 2c

snmp-server contact "Field Support."

snmp-server location "End User Premise."

See Also diag post, diag setcycle, show diag burninstatus, show diag burninstatus

show running-config tacacs-server

Displays a user configuration for the TACACS+ server from the configuration database.

Synopsis show running-config tacacs-server

Operands None

Description Use this command to display the user configuration for the TACACS+ server.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples The following example displays the user configuration for the TACACS+ server.

```
switch# show running-config tacacs-server ?
Possible completions:
   10.xx.xx.xxx IP Address or Hostname of this TACACS+ server
   10.xx.xx.x IP Address or Hostname of this TACACS+ server

switch# show running-config tacacs-server host 10.xx.xx.x
tacacs-server host 10.xx.xx.x
key new#virgo*secret
retries 100
```

See Also radius-server, show running-config radius-server, tacacs-server

show running-config username

Displays user-configured usernames.

Synopsis show running-config username username

Operands username The name of the user.

username Specifies the username associated with the user.

Description Use this command to display usernames.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples The following example displays details about user-configured usernames.

switch# show running-config username testUser

username testUser

desc "add op test user"

password \$1\$no\$password-hidden

role admin enabled false

See Also show users, username, unlock username

show running-config switch-attributes

Displays switch attributes.

Synopsis show running-config switch-attributes [switchID] { chassis-name | host-name }

Operands switchID Specifies the switch ID for which to display the attribute.

chassis-namebost-nameDisplays the switch chassis name.

Defaults Displays all switch attributes on the local switch.

The default chassis name is "VDX6720-24" or "VDX6720-60", depending on the switch model.

The default host name is "sw0"

Command Modes Privileged EXEC mode

Description Use this command to display the switch attributes.

Usage Guidelines There are no usage guidelines for this command.

Examples To display all attributes for switch 2:

```
switch# show running-config switch-attributes 2
switch-attributes 2
chassis-name VDX6720-24
host-name sw0
!
```

To display the host name of the local switch:

```
switch# show running-config switch-attributes host-name
switch-attributes 2
host-name sw0
!
```

See Also switch-attributes

show running-configuration diag post

Displays the current diagnostic power-on self-test (POST) configuration.

Synopsis show running-configuration diag post

Operands None

Description Use this command to display the current configuration of the POST.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples To display the diagnostic POST configuration:

switch(config)# show running-configuration diag post

See Also diag post

show sflow

Displays sFlow configuration information and statistics.

Synopsis show sflow

Operands all Displays all sFlow information and statistics.

interface tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults By default, sFlow is disabled on all interfaces.

Command Modes Privileged EXEC mode

Description Use this command to display sFlow configuration information and statistics.

Usage Guidelines There are no usage guidelines for this command.

Examples To display all sFlow statistics:

switch#show sflow all
sFlow services are enabled
Global default sampling rate: 32768
Global default counter polling interval: 20
1 collectors configured
Collector IP addr: 172.21.162.51, Agent IP addr: 10.32.152.22, UDP port: 6343
77 UDP packets exported
0 UDP packets dropped
165 sFlow samples collect

To display sFlow statistics for a specific interface:

To display sFlow statistics on 10 Gbps Ethernet interface 1/16:

switch#show sflow interface tengigabitethernet 1/16
te 1/16
Configured sampling rate :8192
Actual sampling rate :8192
Counter polling interval :15
Samples rcvd from h/w :33

See Also None

show spanning-tree

Displays all Spanning Tree Protocol information.

Synopsis show spanning-tree vlan vlan_id

Operands vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display all STP information.

Usage Guidelines There are no usage guidelines for this command.

Examples To display all STP information:

```
switch#show spanning-tree
Spanning-tree Mode: Multiple Spanning Tree Protocol
 CIST Root Id: 8000.0005.1e76.1aa0 (self)
 CIST Bridge Id: 8000.0005.1e76.1aa0
 CIST Reg Root Id: 8000.0005.1e76.1aa0 (self)
 CIST Root Forward Delay: 15; Hello Time: 2; Max Age: 20; Max-hops: 20
 Configured Forward Delay: 15; Hello Time: 2; Max Age: 20; Max-hops: 20;
 Tx-HoldCount: 6
 Number of topology change(s): 0
 Bpdu-guard errdisable timeout: disabled
 Bpdu-guard errdisable timeout interval: 300 sec
 Migrate Time: 3 sec
 Port Te 0/0 enabled
    IfIndex: 67108864; Id: 8000; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
     CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
     Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
     Configured Root guard: off; Operational Root guard: off
     Boundary: yes
     Bpdu-guard: off
     Bpdu-filter: off
     Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
 Port Te 0/8 enabled
     IfIndex: 67633408; Id: 8008; Role: Disabled; State: Discarding
     Designated External Path Cost: 0; Internal Path Cost 0
     Configured Path Cost: 2000
     Designated Port Id: 0; CIST Priority: 128
```

```
Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
Port Te 0/19 enabled
    IfIndex: 68354563; Id: 8013; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
Port Te 0/20 enabled
    IfIndex: 68420100; Id: 8014; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
```

See Also show spanning-tree interface

show spanning-tree brief

Displays the status and parameters of the Spanning Tree Protocol.

Synopsis show spanning-tree [vlan vlan_id] brief

Operands vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display a summary of the status and parameters of the Spanning Tree

Protocol for each interface, including the port roles and port states.

The following describes the port roles and states:

Port roles—root port, designated port, alternate port and backup port.

• Port states—discarding, learning, forwarding, and blocked.

Port types—edge port (PortFast), point-to-point, and shared port.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the interface summary of the Spanning Tree Protocol:

switch#show spanning-tree brief

Spanning-tree Mode: Rapid Spanning Tree Protocol

Root ID Priority 32768

Address 0005.1e76.1aa0

Hello Time 2, Max Age 20, Forward Delay 15

Bridge ID Priority 32768

Address 0005.1e76.1aa0

Hello Time 2, Max Age 20, Forward Delay 15, Tx-HoldCount 6

Migrate Time 3 sec

Interface	Role	Sts	Cost	Prio	Link-type	Boundary	Edge
Te 0/0	DIS	DSC	2000	128	P2P	Yes	No
Te 0/1	ALT	BLK	2000	128	P2P	Yes	No
Te 0/2	RTPT	BLK	2000	128	P2P	Yes	No
Te 0/3	DIS	BLK	2000	128	P2P	Yes	No
Te 0/8	DIS	DSC	2000	128	P2P	Yes	No
Te 0/19	DIS	DSC	2000	128	P2P	Yes	No
Te 0/20	DIS	DSC	2000	128	P2P	Yes	No

See Also show spanning-tree interface

show spanning-tree interface

Displays the state of the Spanning Tree Protocol for all named port-channels or 10 Gbps Ethernet interfaces.

Synopsis show spanning-tree interface [port-channel number | tengigabitethernet slot/port]

Operands port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the state of the spanning tree for all named port-channels or 10

Gbps Ethernet interfaces.

Usage Guidelines The following describes the port roles, states and types:

Port roles—root port, designated port, alternate port and backup port.

Port states—discarding, learning, and forwarding.

Port types—edge port (PortFast), point-to-point, and shared port.

Examples To display information on a 10 Gbps Ethernet interface:

```
switch#show spanning-tree interface tengigabitethernet 0/0
Spanning-tree Mode: Rapid Spanning Tree Protocol
```

```
Root Id: 8000.0005.1e76.1aa0 (self)
Bridge Id: 8000.0005.1e76.1aa0
Port Te 0/0 enabled
   IfIndex: 67108864; Id: 8000; Role: Disabled; State: Discarding
    Designated Path Cost: 0
    Configured Path Cost: 2000
    Designated Port Id: 0; Port Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    Number of forward-transitions: 0
    Version Rapid Spanning Tree Protocol - Received None - Send RSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
```

See Also show spanning-tree brief

show spanning-tree mst brief

Displays the status and parameters of the Multiple Spanning Tree Protocol (MSTP) instance information in brief.

Synopsis show spanning-tree mst brief

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the status and parameters of the Multiple Spanning Tree Protocol

(MSTP) instance information. It includes the port roles, port states and port types.

Usage Guidelines The following describes the port roles, states, and types:

Port roles—root port, designated port, alternate port, and backup port.

· Port states—discarding, learning, and forwarding.

Port types—edge port (PortFast), point-to-point, and shared port.

Examples To display the status and parameters of the MSTP instance information:

switch#show spanning-tree mst brief

Spanning-tree Mode: Multiple Spanning Tree Protocol

CIST Root ID Priority 32768

Address 0005.1e76.1aa0

CIST Bridge ID Priority 32768

Address 0005.1e76.1aa0

CIST Regional Root ID Priority 32768

Address 0005.1e76.1aa0

Configured Hello Time 2, Max Age 20, Forward Delay 15

Max Hops 20, Tx-HoldCount 6

CIST Root Hello Time 2, Max Age 20, Forward Delay 15, Max Hops 20

CIST Root path cost 0

Interface	Role	Sts	Cost	Prio	Link-type	Boundary	Edge
Te 0/0	DIS	DSC	2000	128	P2P	Yes	No
Te 0/1	ALT	BLK	2000	128	P2P	Yes	No
Te 0/2	RTPT	BLK	2000	128	P2P	Yes	No
Te 0/3	DIS	BLK	2000	128	P2P	Yes	No
Te 0/8	DIS	DSC	2000	128	P2P	Yes	No
Te 0/19	DIS	DSC	2000	128	P2P	Yes	No
Te 0/20	DIS	DSC	2000	128	P2P	Yes	No

See Also show spanning-tree mst instance, show spanning-tree mst interface

show spanning-tree mst detail

Displays details on an interface for the Multiple Spanning Tree Protocol (MSTP) instance running.

Synopsis show spanning-tree mst detail [interface port-channel number | interface tengigabitethernet

slot/port]

Operands interface Specifies the interface for which to display the spanning-tree information.

port-channel number

Specifies the port-channel of the interface. The range of valid values is from

1 through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults There are no default configuration for this command.

Command Modes Privileged EXEC mode

Description Use this command to display details on a specified interface for the MSTP instance running.

Usage Guidelines There are no usage guidelines for this command.

Examples To display MSTP information on the switch in detail:

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

```
Spanning-tree Mode: Multiple Spanning Tree Protocol
CIST Root Id: 8000.0005.1e76.1aa0 (self)
CIST Bridge Id: 8000.0005.1e76.1aa0
CIST Reg Root Id: 8000.0005.1e76.1aa0 (self)
CIST Root Forward Delay: 15; Hello Time: 2; Max Age: 20; Max-hops: 20
Configured Forward Delay: 15; Hello Time: 2; Max Age: 20; Max-hops: 20;
Tx-HoldCount: 6
Number of topology change(s): 0
Bpdu-guard errdisable timeout: disabled
Bpdu-guard errdisable timeout interval: 300 sec
Migrate Time: 3 sec
CIST Port Details.
============
Instance: 0; Vlans:1, 100
Port Te 0/0 enabled
    IfIndex: 67108864; Id: 8000; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
   Configured Path Cost: 2000
   Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
```

```
CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
Port Te 0/8 enabled
    IfIndex: 67633408; Id: 8008; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
Port Te 0/19 enabled
    IfIndex: 68354563; Id: 8013; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0
Port Te 0/20 enabled
    IfIndex: 68420100; Id: 8014; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
```

2

```
Received BPDUs: 0; Sent BPDUs: 0

MSTI details.
==========
```

See Also show spanning-tree mst instance, show spanning-tree mst interface

show spanning-tree mst instance

Displays information on a specified Multiple Spanning Tree Protocol (MSTP) instance.

Synopsis show spanning-tree mst instance instance_id [interface port-channel number | interface

tengigabitethernet slot/port]

Operands instance_id Specifies the MSTP instance for which to display information. The range of

valid values is from 1 through 15.

interface Specifies the interface for which to display the MSTP instance information.

port-channel number

Specifies the port-channel of the interface. The range of valid values is from

1 through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface for which to display the MSTP

instance information.

slot Specifies a valid slot number for the interface for which to display

information on the MSTP instance.

port Specifies a valid port number for the interface for which to display

information on the MSTP instance.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display information on a specified instance of the MSTP.

Usage Guidelines There are no usage guidelines for this command.

Examples To display information on MSTP instance 1:

switch#show spanning-tree mst instance 1 interface tengigabitethernet 0/0

Instance: 1; VLANs: 100

MSTI Root Id: 8001.0005.1e76.1aa0 (self)
MSTI Bridge Id: 8001.0005.1e76.1aa0

MSTI Bridge Priority: 32768

See Also show spanning-tree mst brief, show spanning-tree mst interface

show spanning-tree mst interface

Displays information for a specified interface for a Multiple Spanning Tree Protocol (MSTP) instance.

Synopsis show spanning-tree mst interface [port-channel number | tengigabitethernet slot/port]

Operands port-channel number

Specifies the port-channel of the interface. The range of valid values is from

1 through 63.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number for the interface for which to display

information for the MSTP instance.

port Specifies a valid port number for the interface for which to display

information for the MSTP instance.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display MSTP protocol specific information such as Common and Internal

Spanning Tree (CIST) spanning-tree related information, information to each MSTP instance

(MSTI), and the state of the port specific to each MSTI.

Usage Guidelines There are no usage guidelines for this command.

Examples To display information for the MSTP interface:

```
switch#show spanning-tree mst interface tengigabitethernet 0/0
```

```
Spanning-tree Mode: Multiple Spanning Tree Protocol
```

```
CIST Root Id: 8000.0005.1e76.1aa0 (self)
CIST Bridge Id: 8000.0005.1e76.1aa0
CIST Reg Root Id: 8000.0005.1e76.1aa0 (self)

CIST Operational Port Hello Time: 0
Number of forward-transitions: 0
Version: Multiple Spanning Tree Protocol - Received None - Send MSTP Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
Configured Root guard: off; Operational Root guard: off
Boundary: yes
Bpdu-guard: off
Bpdu-filter: off
Link-type: point-to-point
Received BPDUs: 0; Sent BPDUs: 0
```

Instance Role Sts Cost Prio VLANs

O DIS DSC 2000 128 1

See Also show spanning-tree brief, show spanning-tree mst brief

show startup-config

Displays the contents of the startup configuration.

Synopsis show startup-config

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the contents of the startup configuration.

Usage Guidelines This command is supported only on the local switch.

Examples To display the startup configuration:

```
switch# show startup-config
logging switchid 2
raslog console INFO
logging syslog ipaddress [ ]
switch-attributes 2
chassis-name chassis
host-name sw
support switchid 2
ffdc
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr
 rw
!
snmp-server community "Secret COde"
snmp-server community common
snmp-server community private
 rw
[output truncated]
```

See Also copy, copy running-config startup-config, delete, dir, chassis disable, show file, show support, vcs

show startup-config fcoe

Displays the startup configuration for an FCoE interface.

Synopsis show startup-config fcoe fabric-map default

Operands None

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Description This command displays the current startup configuration for FCoE. This is not neccessarily the

same as the running configuration.

Usage Guidelines There are no usage guidelines for this command.

Examples switch#show startup-config fcoe fabric-map

fcoe

fabric-map default
 vlan-id 1002
 virtual-fabric 1
 priority 3
 fcmap 0E:FC:00

advertisement interval 8000

keep-alive timeout

See Also None

show statistics access-list mac

Shows active ACL rules in the switch and if the rules have counters enabled.

Synopsis

show statistics access-list mac name [[std_acl | ext_acl] interface port-channel number | [std_acl | ext_acl] interface tengigabitethernet slot/port | [std_acl | ext_acl] interfacevlan vlan_id]

Operands

name Specifies a unique name for the MAC ACL.

std_acl Specifies the output should be for the standard ACLs.ext_acl Specifies the output should be for the extended ACLs.

interface port-channel number

Specifies the port-channel number. The range of valid values is from 1

through 63.

interface tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number.

interface vlan vlan_id

Specifies the VLAN number. The range of valid values is from 1 through

3583.

Defaults

There are no default configurations for this command.

Command Modes

Privileged EXEC mode

Description

Use this command to display the active rules on the switch and whether those rules have counters

Examples

To display the statistics for standard and extended MAC ACL applied on two interfaces tengigabitethernet 0/1 and VLAN 100:

```
switch#show statistics access-list mac std_acl mac access-list standard std_acl on interface Te 0/1
```

```
seq 10 deny 0011.2222.3333 count (6312 frames)
seq 20 deny 0011.2222.4444 count (20 frames)
seq 30 deny 0011.2222.5555
seq 40 deny 0011.2222.6666 count (100000 frames)
```

${\tt switch\#show}$ statistics access-list mac ext_acl mac access-list extended ext_acl on interface VI 100

```
seq 10 deny 0011.2222.2222 0022.2222.2222 ipv4 count (4350 frames)
seq 20 deny 0011.2222.2222 0022.2222.2222 fcoe count (0 frames)
seq 30 deny 0011.2222.2222 0022.2222.2222 arp
seq 40 deny 0011.2222.2222 0022.2222.2222 10000 count (560 frames)
```

If the rule is not written into the hardware the output displays as shown below:

```
seq 8 permit 00c0.e000.0080 count (unwritten)
```

If the rule is written into the hardware, but the counters are not enabled for that rule, the output displays as shown below:

seq 9 permit 00c0.e000.0090 count (uncounted)

See Also show running-config, show mac access-group

show support

Displays a list of core files on the switch.

Synopsis show support [switchid { switchID | all }]

Operands switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchID Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults Displays information for the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display a list of core files on the switch.

Usage Guidelines Pagination is not supported with the **all** option.

Examples To display the core files:

switch#show support

No core or FFDC data files found!

See Also clear support, copy support, firmware download, firmware restore, interface management, vcs

show system

Displays system information.

Synopsis show system

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display system information of hardware and software details.

Usage Guidelines There are no usage guidelines for this command.

Examples To display the system information:

```
switch#show system
```

```
Stack MAC
                  : 00:05:1E:76:42:00
  -- UNIT 0 --
Unit Name
                   : switch
Status : Online
Hardware Rev : 76.6
FC Port(s)
                  : 8
Tengig Port(s) : 24
Up Time : 18:28:27 up 4:09 FOS Version : v6.1.2
Jumbo Capable : yes
Burned In MAC : 00:05:1E:76:42:00
Management IP : 10.35.155.204
Status
  -- Power Supplies --
PS0 is OK
PS1 is OK
  -- Fan Status --
Fan 1 is Ok
Fan 2 is Ok
Fan 3 is Ok
```

See Also show environment, show version

show tech-support

Displays output for troubleshooting.

Synopsis show tech-support

Operands None

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to run a script that automatically runs a variety of **show** commands with output

that is useful to Technical Support for troubleshooting.

Usage Guidelines There are no usage guidelines for this command.

Examples To display output for troubleshooting:

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

```
----- date -----
Thu Feb 19 18:30:13 UTC 2009
-----show version -----
Fabric Operating System Software
Fabric Operating System Version: 6.1
Copyright (c) 1995-2008 Brocade Communications Systems, Inc.
Build Time: 03:35:17 Feb 18, 2009
switch uptime: 04:11:09
Firmware name: v6.1.2
Switch Model Name: Brocade 8000
Control Processor: Freescale Semiconductor 8548E with 1016 MB of memory
4MB of boot flash memory.
 8 FC Port(s)
 24 Ten GigabitEthernet/IEEE 802.3 interface(s)
----- show running-config -----
switch#
```

See Also None

show users

Displays the current state of all the users logged into the system.

Synopsis show users

Operands None

Description Displays active user sessions and locked user accounts.

Defaults There are no defaults for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples switch# show users

USER SESSIONS

RBridge

ID Username Host IP Devic Time Logged In
e

1 root 0.0.0.0 con0 2010-09-30 01:57:23

1 user 10.70.4.105 vty/0 2010-09-30 01:57:41

LOCKED USERS

RBridge
ID Username
1 user

See Also show running-config username, username, unlock username

show vcs

Displays details of the VCS configuration.

NOTE

The **show vcs** command returns the state as "disabled" if the switch is in standalone mode. The **show fabric all** command cannot be issued in standalone mode.

Synopsis show vcs

Operands None

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

mode.

Usage Guidelines The VCS ID and switch RBridge ID are displayed only in VCS-enabled mode.

Examples If vcs is enabled, the following verbiage displays:

switch# show vcs
state : Enabled
vcsid : 1
rbridgeid : 21

If VCS functionality is disabled, the following output displays:

switch# show vcs
state : Disabled

See Also diag setcycle, vcs

show version

Displays the firmware version.

Synopsis show version [brief][switchid { switchid | all }]

Operands brief Displays the firmware version only.

switchid Executes the command on the specified switches. Valid completions for

switchid include the following:

switchid Specifies the switch ID.

all Specifies all switches in the fabric.

Defaults Displays local switch information.

Command Modes Privileged EXEC mode

Description Use this command to display firmware version information and build dates. The command output includes the following:

Network Operating System Version - The firmware version number

- Build Time The build date and time of the firmware
- Firmware name The label of the firmware image
- Control Processor Control Processor model and memory

Usage Guidelines There are no usage guidelines for this command.

Examples To display the firmware version information:

switch#show version

To display the brief version only:

switch#show version brief

v2.0.0

Appl	Primary/Secondary	Versions
NOS	v2.0.0	

See Also vcs, firmware download, firmware restore, interface management

show vlan

Displays information about a specific VLAN interface.

Synopsis show vlan [vlan_id | brief | classifier]

Operands vlan_id Specifies the VLAN interface to display. The range of valid values is from 1

through 3583.

brief Specifies to display VLAN information for all interfaces including static and

dynamic.

classifier Specifies to display all VLAN classification information.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display information about VLAN.

Usage Guidelines There are no usage guidelines for this command.

Examples To show information on a VLAN:

switch#show vlan 1

VLAN Name State Ports

(u)-Untagged, (t)-Tagged

(c)-Converged

default ACTIVE Te 0/0(t) Te 0/4(t) Te 0/5(t)

Te 0/8(t) Te 0/10(t) Te 0/11(c)

Po 1(t) Po 63(t)

See Also None

show vlan classifier

Displays information about a specific VLAN classifier group.

Synopsis show vlan classifier [group number | interface group number | port-channel number | rule

number | tengigabitethernet slot/port | vlan vlan_id]

Operands group number Specifies the VLAN classifier group number. The range of valid values is from

from 1 through 16.

interface group number

Specifies the VLAN classifier interface group number. The range of valid

values is from 1 through 16.

port-channel number

Specifies the VLAN classifier port-channel number. The range of valid values

is from 1 through 63.

rule number Specifies the VLAN classifier rule number. The range of valid values is from 1

through 256.

tengigabitethernet

Specifies a valid 10 Gbps Ethernet interface.

slot Specifies a valid slot number.

port Specifies a valid port number

vlan vlan_id Specifies the VLAN to display. The range of valid values is from 1 through

3583.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Description Use this command to display information about all configured VLAN classifier groups or a specific

VLAN interface group.

Usage Guidelines If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is

specified, a specific configured VLAN classifier group is shown.

Examples To display the VLAN classifier for group 1:

switch#show vlan classifier group 1
vlan classifier group 1 rule 1

See Also None

shutdown

Disables the selected interface.

Synopsis shutdown

no shutdown

Operands None

Defaults The interface is disabled.

Command Modes Interface configuration mode

Description Use this command to disable an interface.

Usage Guidelines Use the **no shutdown** version of the command to enable the interface.

Examples To disable an interface:

switch(conf-if-te-0/1)#shutdown

To enable an interface:

switch(conf-if-te-0/1)#no shutdown

See Also interface, show ip interface, show interface

shutdown (STP)

Disables the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or the Spanning Tree Protocol (STP) globally.

Synopsis shutdown

no shutdown

Operands None

Defaults STP is not required in a loop-free topology and is not enabled by default.

Command Modes Protocol Spanning Tree mode

Description Use this command to disable the MSTP, RSTP, or STP globally.

Use the no shutdown version of the command to enable MSTP, RSTP, or STP.

Examples To disable STP globally:

switch(config)#protocol spanning-tree rstp

 $\verb|switch(conf-rstp)| \# \textbf{shutdown}|$

To enable STP globally:

switch(config)#protocol spanning-tree rstp

switch(conf-rstp)#no shutdown

See Also None

snmp-server community

Sets or removes the community string and read-write or read-only access for each community.

Synopsis snmp-server community string [ro|rw]

no snmp-server community string [ro | rw]

Operands string Specifies the community string.

ro|rw Sets the read-only or read-write access for each community.

Description Use this command to manage the configuration of the SNMP agent in the switch. The

configuration includes SNMPv1 and SNMPv2c configuration settings.

Defaults There are six default community strings configured for the user: three read-write strings and three

read-only strings. The community strings on a read-write group are "Secret Code," "OrigEquipMfr," and "private." The three read-only community strings are "public," "common," and "Converged

Network."

If no access is specified, read only (ro) is the default.

NOTE

You can specify one of the six default community strings when the system first comes up. If you create a new community string, you must delete one of the six default strings to make space for the new community string.

Command Modes Global configuration mode

Usage Guidelines There are no usage guidelines for this command.

Examples To remove the community string "public":

switch(config)# no snmp-server community public

To add user123 with read-only access to the user's list for v1 and v2c:

switch(config)# snmp-server community user123 ro

To change the access of a read-only community string (user123) to read-write:

switch(config)# snmp-server community user123 rw

See Also show running-config snmp-server, diag setcycle, show diag burninstatus, show diag burninstatus

snmp-server contact

Sets the SNMP server contact string.

Synopsis snmp-server contact string

Operands string Specifies the server contact string.

Description Use this command to set the SNMP server contact string.

Defaults The default contact string is *Field Support*.

Command Modes Global configuration mode

Usage Guidelines There are no usage guidelines for this command.

Examples To set the SNMP server contact string to "Operator 12345":

switch(config)# snmp-server contact "Operator 12345"

To set the SNMP server contact string to the default of "Field Support":

switch(config)# no snmp-server contact

See Also show running-config snmp-server, diag post, show diag burninstatus

snmp-server host

Sets the trap destination IP addresses, version, community string (for v1 and v2c), and destination port for the SNMP server host.

Synopsis snmp-server host ipv4_host community-string [version {1 | 2c }] [udp-port port]

Operands ipv4_host Specifies the IP address of the host (only IPv4 hosts are supported).

community-string Associates a community string with the trap destination.

version 1 | 2c Selects version 1 or 2c traps to be sent to the specified trap host.

udp-port port
Specifies the UDP port where SNMP traps will be received. The default port

is 162. The acceptable range of ports is 0 through 65535.

Description Use this command to set the trap destination IP addresses and SNMP version, to associate a

community string with a trap host community string (for v1 and v2c), and to specify the UDP

destination port where SNMP traps will be received.

Defaults The default UDP port is 162. The default SNMP version is 1.

Command Modes Global configuration mode

Usage Guidelines To configure SNMP trap hosts associated with community strings, you must create the community string using the **snmp-server community** command before configuring the host.

The agent supports six communities and their associated trap recipients and trap recipient severity levels. The default value for the trap recipient of each community is 0.0.0.0. The length of the community string should be in the range of 2 to 16 characters. The default values for the community strings are:

- <community:WORD> Community strings used to query MIB objects.
- ConvergedNetwork—read-only
- OrigEquipMfr—read-write
- Secret C0de—read-write
- common—read-only
- private—read-write
- public—read-only

NOTE

To add any new community string for SNMPv1 or v2c under one of the read-only or read-write groups, one of the six entries listed above must be deleted.

Examples

The following example associates "commaccess" as a read-only community and sets 10.32.147.6 as a trap recipient with SNMP version 2c on target port 162.

switch(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port 162

See Also show running-config snmp-server, diag post, show diag burninstatus, show diag burninstatus

snmp-server location

Sets the SNMP server location string.

Synopsis snmp-server location string

no snmp-server location string

Operands string Specifies the SNMP server location string

Description Use this command to set the SNMP server location string.

Defaults By default the location is set to "End User Premise."

Command Modes Global configuration mode

Usage Guidelines There are no usage guidelines for this command.

Examples To set the SNMP server location string to "Building 3, Room 214":

switch(config)# snmp-server location "Building 3 Room 214"

To set the SNMP server location to the default "End User Premise":

switch(config)# no snmp-server location

See Also show running-config snmp-server, diag post, diag setcycle, show diag burninstatus

spanning-tree autoedge

Enables automatic edge detection.

Synopsis spanning-tree autoedge

no spanning-tree autoedge

Operands None

Defaults Auto-detection is not enabled.

Command Modes Interface configuration mode

Description Use this command to automatically identify the edge port.

Usage Guidelines The port can become an edge port if no Bridge Protocol Data Unit (BPDU) is received.

Use the **no spanning-tree autoedge** command to disable automatic edge detection.

Examples To enable automatic edge detection:

switch(conf-if-te-0/1)#spanning-tree autoedge

See Also protocol spanning-tree

spanning-tree bpdu-mac

Sets the MAC address of the BPDU.

Synopsis spanning-tree bpdu-mac 0100.0ccc.cccd

no spanning-tree bpdu-mac 0100.0ccc.cccd

Operands None

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description Use this command to explicitly set the MAC address of the BPDU. This command will only take

effect when the protocol is PVST or RPVST.

Usage Guidelines This command has no usage guidelines.

Examples None

See Also None

spanning-tree cost

Changes an interface's spanning-tree port path cost.

.Synopsis spanning-tree cost cost [vlan vlan_id]

Operands cost Specifies the path cost for the Spanning Tree Protocol (STP) calculations. The

range of valid values is from 1 through 20000000.

vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults The default path cost is 20000000.

Command Modes Interface configuration mode

Description Use this command to configure the path cost for spanning-tree calculations.

Usage Guidelines Lower path cost indicates a greater chance of becoming root.

Examples To set the port cost to 128:

switch(conf-if-te-0/1)#spanning-tree cost 128

See Also show spanning-tree

spanning-tree edgeport

Enables the edge port on an interface to allow the interface to quickly transition to the forwarding state.

Synopsis spanning-tree edgeport [bpdu-filter | bpdu-guard]

Operands bpdu-filter Sets the edge port Bridge Protocol Data Unit (BPDU) filter for the port.

bpdu-guard Guards the port against the reception of BPDUs.

Defaults Edge port is disabled.

Command Modes Interface configuration mode

Description Use this command to enable the edge port feature. This command is only for RSTP and MSTP. Use

the spanning-tree portfast command for STP.

Usage Guidelines Note the following details about edge ports and their behavior:

A port can become an edge port if no BPDU is received.

- A port must become an edge port before it receives a BPDU.
- When an edge port receives a BPDU, it becomes a normal spanning-tree port and is no longer an edge port.
- Because ports directly connected to end stations cannot create bridging loops in the network, edge ports directly transition to the forwarding state, and skip the listening and learning states

Examples To er

To enable a port to quickly transition to the forwarding state:

```
switch(conf-if-te-0/1)#spanning-tree edgeport
```

To set the edgeport BPDU filter for the port:

```
switch(conf-if-te-0/1)#spanning-tree edgeport
switch(conf-if-te-0/1)#spanning-tree edgeport bpdu-filter
```

To guard the port against reception of BPDUs:

```
switch(conf-if-te-0/1)#spanning-tree edgeport
switch(conf-if-te-0/1)#spanning-tree edgeport bpdu-guard
```

See Also

spanning-tree portfast, spanning-tree autoedge

spanning-tree guard root

Enables the guard root to restrict which interface is allowed to be the spanning-tree root port or the

path-to-the root for the switch.

Synopsis spanning-tree guard root vlan_id

no spanning-tree guard root

Operands *vlan_id* Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults Guard root is disabled.

Command Modes Interface configuration mode

Description Use this command to enable the guard root on the interface. Use the **no spanning-tree guard root**

command to disable guard root on the selected interface.

Usage Guidelines The root port provides the best path from the switch to the root switch.

Guard root protects the root bridge from malicious attacks and unintentional misconfigurations where a bridge device that is not intended to be the root bridge becomes the root bridge. This causes severe bottlenecks in the datapath. Guard root ensures that the port on which it is enabled is a designated port. If the guard root enabled port receives a superior Bridge Protocol Data Unit

(BPDU), it goes to a discarding state.

Examples To enable guard root:

switch(conf-if-te-0/1)#spanning-tree guard root

See Also spanning-tree cost

spanning-tree hello-time

Configures the hello-time in seconds on the interface.

Synopsis spanning-tree hello-time seconds

no spanning-tree hello-time

Operands seconds Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent

by the root switch configuration messages. The range of valid values from 1

to 10.

Defaults The default is 2 seconds.

Command Modes Interface configuration mode

Description Use this command to set the interval time between the BPDUs sent by the root switch. Use the **no**

spanning-tree hello-time command to return to the default setting. This command is only for MSTP.

Usage Guidelines Changing the hello-time affects all spanning-tree instances. The max-age command setting must

be greater than the hello-time command setting.

Examples To set the hello time to 5 seconds:

switch(conf-if-te-0/1)#spanning-tree hello-time 5

See Also forward-delay, max-age, show spanning-tree

spanning-tree instance

Sets restrictions for the port of particular MSTP instances.

Synopsis spanning-tree instance instance_id [cost cost | priority | priority | restricted-role | restricted-tcn]

no spanning-tree instance instance_id

Operands instance_id Specifies the MSTP instance. The range of valid values is from 1 through 15.

cost cost Specifies the path-cost for a port. The range of valid values is from 1 through

20000000.

priority priority Specifies the port priority for a bridge in increments of 16. The range of valid

values is from 0 through 240.

restricted-role Specifies to restrict the role of a port.

restricted-tcn Specifies to restrict the propagation of the topology change notifications

from a port.

Defaults The default path-cost value is 2000 on a 10 Gbps Ethernet interface.

Command Modes Interface configuration mode

Description Use this command to set restrictions for a port on a particular MSTP instance.

Usage Guidelines Use this command for MSTP-specific configurations.

Use the **no spanning-tree instance** *instance_id* command to remove the instance.

Examples To set restrictions for the port of MSTP instance 1 with the cost of 40000:

switch(conf-if-te-0/1)#spanning-tree instance 1 cost 40000

See Also instance, show spanning-tree

spanning-tree link-type

Enables and disables the rapid transition for the Spanning Tree Protocol.

Synopsis spanning-tree link-type [point-to-point | shared]

Operands point-to-point Enables rapid transition.

shared Disables rapid transition.

Defaults The default is point-to-point.

Command Modes Interface configuration mode

Description Use this command to specify a link type for the Spanning Tree Protocol.

Usage Guidelines This command overrides the default setting of the link type.

Examples To specify the link type as shared:

switch(conf-if-te-0/0)#spanning-tree link-type shared

See Also spanning-tree link-type

spanning-tree portfast

Enables the Port Fast feature on an interface to allow the interface to quickly transition to

forwarding state.

Synopsis spanning-tree portfast [bpdu-filter | bpdu-guard]

Operands bpdu-filter Sets the Port Fast BPDU filter for the port.

bpdu-guard Guards the port against the reception of BPDUs.

Defaults Port Fast is disabled.

Command Modes Interface configuration mode

Description Use this command to enable the Port Fast feature. This command is is the only for the STP. Port

Fast immediately puts the interface into the forwarding state without having to wait for the standard forward time. Use the **spanning-tree edgeport** command for MSTP and RSTP.

Usage Guidelines If you enable spanning-tree portfast bpdu-guard on an interface and the interface receives a

BPDU, the software disables the interface and puts the interface in the ERR_DISABLE state.

Examples To enable a port to quickly transition to the forwarding state:

switch(conf-if-te-0/1)#spanning-tree portfast

To set the Port Fast BPDU filter for the port:

switch(conf-if-te-0/1)#spanning-tree portfast bpdu-filter

To guard the port against the reception of BPDUs:

switch(conf-if-te-0/1)#spanning-tree portfast bpdu-guard

See Also spanning-tree portfast, spanning-tree autoedge

spanning-tree priority

Changes an interface's spanning-tree port priority.

Synopsis spanning-tree priority priority [vlan vlan_id]

no spanning-tree priority

Operands priority Specifies the interface priority for the spanning tree. The range of valid

values is from 0 through 240. Port priority is in increments of 16.

vlan vlan_id Specifies the VLAN number. The range of valid values is from 1 through

4094.

Defaults The default value is 128.

Command Modes Interface configuration mode

Description Use this command to change an interface's spanning-tree port priority. Use the no spanning-tree

priority command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To configure the port priority to 16:

switch(conf-if-te-0/1)#spanning-tree priority 16

See Also spanning-tree cost, show spanning-tree

spanning-tree restricted-role

Restricts the role of the port from becoming a root port.

Synopsis spanning-tree restricted-role

no spanning-tree restricted-role

Operands None

Defaults The restricted role is disabled.

Command Modes Interface configuration mode

Description Use this command to configure the port from becoming a root port. Use the **no spanning-tree**

restricted-role command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To configure the port from becoming a root port:

switch(conf-if-te-0/1)#spanning-tree restricted-role

See Also show spanning-tree

spanning-tree restricted-tcn

Restricts the topology change notification Bridge Protocol Data Units (BPDUs) sent on the port.

Synopsis spanning-tree restricted-tcn

no spanning-tree restricted-tcn

Operands None

Defaults The restricted TCN is disabled.

Command Modes Interface configuration mode

Description Use this command to restrict the topology change notification Bridge Protocol Data Units (BPDUs)

sent on the port.

Use the no spanning-tree restricted-tcn command to disable this option.

Examples To restrict the TCN on a specific interface:

 $\verb|switch(conf-if-te-0/1)| \verb|#spanning-tree| restricted-tcn| \\$

See Also show spanning-tree

spanning-tree shutdown

Enables or disables spanning tree on the interface.

Synopsis spanning-tree shutdown

no spanning-tree shutdown

Operands None

Defaults Spanning tree is not enabled.

Command Modes Interface configuration mode

Description Use this command to disable spanning tree on the interface or VLAN. Use the no spanning-tree

shutdown command to enable spanning tree on the interface or VLAN.

Once all of the interface ports have been configured for a VLAN, you can enable spanning tree protocol (STP) for all members of the VLAN with a single command. Whichever protocol is currently

selected is used by the VLAN. Only one type of STP can be active at a time.

A physical interface port can be a member of multiple VLANs. For example, a physical port can be a member of VLAN 1002 and VLAN 55 simultaneously. In addition, VLAN 1002 can have STP

enabled and VLAN 55 can have STP disabled simultaneously.

Usage Guidelines There are no usage guidelines for this command.

Examples To disable spanning tree on a specific interface:

switch(config)#interface tengigabitethernet 0/1
switch(conf-if-te-0/1)#spanning-tree shutdown

To enable spanning tree on VLAN 1002:

switch(config)#interface vlan 1002
switch(conf-if-vl-1002)#no spanning-tree shutdown

See Also protocol spanning-tree

spanning-tree tc-flush-standard

Flushes the Media Access Control (MAC) address based on the optimal scheme.

Synopsis spanning-tree tc-flush-standard

no spanning-tree tc-flush-standard

Operands None

Defaults MAC address flushing is enabled.

Command Modes Global configuration mode

Description Use this command to flush the MAC address based on the optimal scheme. Use the **no**

spanning-tree to-flush-standard command to disable the MAC address flushing.

Usage Guidelines There are no usage guidelines for this command.

Examples To disable the MAC address flushing upon receiving any topology change notification:

 $\verb|switch(config)| \verb|#no spanning-tree tc-flush-standard|\\$

See Also show spanning-tree brief

speed

Sets the speed on the interface.

Synopsis speed [10000 | auto]

Operands 10000 Forces the speed to 10 Gbps.

auto Allows the interface to negotiate the speed setting.

Defaults The default setting for this command is **auto**.

Command Modes Interface configuration mode

Description Use this command to set the speed negotiation value for the interface.

Usage Guidelines The speed command is available only for tengigabitethernet ports. The speed for 10 Gbs ports is

fixed at 10000 and cannot be changed).

Examples switch(conf-if-int-0/1)#speed 10000

See Also None

2

support

Enables or disables the first-fault data capture (FFDC).

Synopsis support switchid switchID ffdc

no support switchid switchID ffdc

Operands switchid switchID Executes the command on a switch specified by its switch ID.

ffdc Enables FFDC.

Defaults FFDC is enabled by default.

Command Modes Global configuration mode

Description Use this command enable FFDC. Use the **no** option to disable the feature. When disabled, the

daemon does not capture any data, even when a message with FFDC attributes is logged.

Usage Guidelines There are no usage guidelines for this command.

Examples To enable FFDC:

switch(config)#support switchid 122 ffdc

To disable FFDC:

switch(config)# no support switchid 122 ffdc

See Also clear support, copy support, show support

switch-attributes

Sets switch attributes.

Synopsis switch-attributes switchID { chassis-name string | host-name string }

Operands switchID Specifies the switch ID for which to set the attribute.

 $\begin{tabular}{ll} \textbf{chassis-name} & string & Sets the switch chassis name. \\ \end{tabular}$

host-name string Sets the switch host name.

Defaults The default chassis name is "VDX6720-24" or "VDX6720-60", depending on the switch model.

The default host name is "sw0"

Command Modes Global configuration mode

Description Use this command to set the switch attributes.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the host name for switch 2:

switch(config)# switch attributes 2 host-name VDX7620-24

See Also show running-config switch-attributes

2

switchport

Puts the interface to Layer 2 mode and sets the switching characteristics of the Layer 2 interface

to the defaults.

Synopsis switchport

no switchport

Operands None

Defaults By default, all Layer 2 interfaces are mapped to default VLAN 1 and the interface is set to access

mode.

Command Modes Interface configuration mode

Description Use this command to set the switching characteristics of the Layer 2 interface. Use the **no**

switchport command to take the switch out of the Layer 2 mode.

Usage Guidelines For changing the interface configuration mode to trunk or changing the default VLAN mapping, use

additional switchport commands.

Examples To put an interface in Layer 2 mode:

switch(conf-if-te-0/1)#switchport

To remove an interface from Layer 2 mode:

switch(conf-if-te-0/1)#no switchport

See Also show vian, switchport mode, switchport access, switchport trunk

switchport access

Sets the Layer 2 interface as access.

Synopsis switchport access vlan vlan_id

no switchport access vlan

Operands vlan vlan_id Sets the port VLAN (PVID) to the specified vlan_id. The range of valid values

is from 1 through 3583.

Defaults By default, all Layer 2 interfaces are in access mode and belong to the VLAN ID 1.

Command Modes Interface configuration mode

Description Use this command to set the Layer 2 interface as access. In access mode, the interface only

allows untagged and priority tagged packets. Use the no switchport access vian command to set

the PVID to the default VLAN 1.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the Layer 2 interface PVID to 100:

switch(conf-if-te-0/19)#switchport access vlan 100

See Also show vlan, switchport mode, switchport trunk

switchport mode converged

Adds or removes native and tagged VLANs on a Layer 2 interface.

Synopsis switchport mode converged [vlan vlan_id | allowed vlan [add vlan_id | all | except vlan_id | none

| remove vlan_id]]

no switchport mode converged

Operands vlan vlan_id Sets the default native VLAN for the Layer 2 interface.

allowed vian Sets the VLANs that will transmit and receive through the Layer 2 interface.

add vlan_id Adds a VLAN to transmit and receive through the Layer 2 interface. The

range of valid values is from 2 through 3583.

all Allows all VLANs to transmit and receive through the Layer 2 interface.

except vlan_id Allows all VLANs except the VLAN ID to transmit and receive through the

Layer 2 interface. The range of valid values is from 2 through 3583.

none Allows no VLANs to transmit and receive through the Layer 2 interface.

remove vlan_id Removes a VLAN that transmits and receives through the Layer 2 interface.

The range of valid values is from 2 through 3583.

Defaults The default native VLAN for a converged interface is 1.

Command Modes Interface configuration mode

Description Use this **no switchport mode converged** command to add or remove tagged VLANs on a Layer 2

interface.

Usage Guidelines Use the command to disable this option.

Examples To set the native VLAN of 200 on an interface:

switch(conf-if-te-0/19)#switchport mode converged vlan 200

To set the tagged VLAN on an interface to 100:

switch(conf-if-te-0/19)#switchport mode converged allowed vlan add 100

To remove the tagged VLAN 100 from the interface:

switch(conf-if-te-0/19)#switchport mode converged allowed vlan remove 100

See Also show vlan, switchport mode, switchport trunk

switchport mode

Sets the mode of the Layer 2 interface.

Synopsis switchport mode [access | trunk | converged]

Operands access Sets the Layer 2 interface as access.

trunk Sets the Layer 2 interface as trunk.

converged Sets the Layer 2 interface as converged.

Defaults There are no defaults for this command.

Command Modes Interface configuration mode

Description Use this command to set the mode of the Layer 2 interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the mode of the interface to access:

switch(conf-if-te-0/19)#switchport mode access

To set the mode of the interface to trunk:

switch(conf-if-te-0/19)#switchport mode trunk

To set the mode of the interface to converged:

switch(conf-if-te-0/19)#switchport mode converged

See Also show vlan, switchport trunk

switchport trunk

Adds or removes tagged VLANs on a Layer 2 interface.

Synopsis switchport trunk allowed vlan [add vlan_id | all | except vlan_id | none | remove vlan_id]

Operands allowed vlan Sets the VLANs that will transmit and receive through the Layer 2 interface.

add vlan_id Adds a VLAN to transmit and receive through the Layer 2 interface. The

range of valid values is from 2 through 3583.

all Allows all VLANs to transmit and receive through the Layer 2 interface.

except vlan_id Allows all VLANs except the VLAN ID to transmit and receive through the

Layer 2 interface. The range of valid values is from 2 through 3583.

none Allows no VLANs to transmit and receive through the Layer 2 interface.

remove *vlan_id* Removes a VLAN that transmits and receives through the Layer 2 interface.

The range of valid values is from 2 through 3583.

Defaults There are no default configurations for this command.

Command Modes Interface configuration mode

Description Use this command to add or remove tagged VLANs on a Layer 2 interface.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the tagged VLAN on an interface to 100:

switch(conf-if-te-0/19)#switchport truck allowed vlan add 100

To remove the tagged VLAN 100 from the interface:

switch(conf-if-te-0/19)#switchport truck allowed vlan remove 100

See Also show vlan, switchport mode, switchport trunk

system-description

Sets the global system description specific to LLDP.

Synopsis system-description line

no system-description

Operands line Specifies a description for the LLDP system. The valid value is a maximum of

50 characters.

Defaults There are no default configurations for this command.

Command Modes Protocol LLDP configuration mode

Description Use this command to set the global system description specific to LLDP. Use the **no**

system-description command to clear the global LLDP system description.

Usage Guidelines There are no usage guidelines for this command.

Examples To set the global system description specific to LLDP:

switch(conf-lldp)#system-description Brocade

See Also system-name

system-name

Sets the global system name specific to LLDP.

Synopsis system-name name

Operands name Specifies a system name for the LLDP. The valid value is a maximum of 32

characters.

Defaults By default, the host name from the switch is used.

Command Modes Protocol LLDP configuration mode

Description Use this command to set the global system name specific to LLDP.

Usage Guidelines There are no usage guidelines for this command.

Examples To specify a system name for the LLDP:

switch(conf-lldp)#system-name Brocade

See Also system-description

tacacs-server

Applies attributes to the TACACS+ server.

Synopsis tacacs-server host <nostname> | <ip-address> [port port] [protocol chap | pap] [key shared

secret key] [timeout secs] [retries num]

no tacacs-server < hostname | ip-address >

Operands host Identifies the TACACS+ server by host name or IP address.

hostname Specifies the domain name of the TACACS+ server.

ip-address Specifies the IP address of the TACACS+ server. Only IPv4 is supported.

port The authentication port.

port Specifies the TCP port used to connect the TACACS+ server for

authentication. The default is 49.

protocol The authentication protocol to be used.

chap | pap Specifies the authentication protocol. Options include CHAP and PAP. The

default is CHAP.

key The shared secret between the switch and the TACACS+ server.

shared_secret_key

The text string that is used as the shared secret between the switch and the

TACACS+ server to make the message exchange secure. The default is

sharedsecret.

timeout The time to wait for the TACACS+ server to respond.

secs Specifies the timeout value, in seconds. The default is 5 seconds.

retries The number of times the switch tries to connect to a TACACS+ server.

num Specifies the number of tries to connect to a TACACS+ server. The default is

5 attempts.

Description Use this command to configure attributes on the TACACS+ server.

Defaults Following are the default values of the global settings:

host—There is no default for the host.

port—TCP port 49

protocol—CHAP

• key-sharedsecret

timeout—3

• retries-5

Command Modes Global configuration mode

Using the no form of the tacacs-server command sets the default values of the individual

attributes.

Examples The following example adds a TACACS+ server:

```
switch(config)# tacacs-server ?
Possible completions:
  <hostname: IP Address of this TACACS+ server>
switch(config)# tacacs-server host 10.24.65.6 ?
Possible completions:
         TCP Port for Authentication (default 49)
 port
 protocolAuthentication protocol to be used (overrides default)
 retriesNumber of retries for this server connection (overrides default)
 timeoutWait time for this server to respond (overrides default)
switch(config)# tacacs-server host 10.24.65.6
switch(config)# tacacs-server host 10.24.65.6 protocol pap ?
Possible completions:
         TCP Port for Authentication (default 49)
 port
 retriesNumber of retries for this server connection (overrides default)
 timeoutWait time for this server to respond (overrides default)
switch(config)# tacacs-server host 10.24.65.6 protocol chap
switch(config)# tacacs-server host 10.24.65.6 protocol chap retries ?
Possible completions:
  <unsignedInt, <= 100, >= 0>
switch(config)# tacacs-server host 10.24.65.6 protocol chap retries 100 switch
(config-tacacs-server-10.24.65.6)#
switch(config)# tacacs-server host 10.38.37.180 protocol chap key
"new#virgo*secret
```

See Also radius-server, show running-config radius-server, show running-config tacacs-server

terminal length

Sets the terminal display length.

Synopsis terminal length *number_of_lines*

Operands *number_of_lines* Specifies the number of lines to be displayed.

Defaults The default display setting is 24 lines.

Command Modes Privileged EXEC mode

Description Use this command to control pagination on the switch. The number of lines setting determines

how many lines will be displayed before a page break occurs.

Usage Guidelines Press the spacebar to display the next page.

Examples To set the display length to 30 lines:

switch# terminal length 30

See Also line vty exec-timeout

terminal monitor

Displays the RASlog and debug outputs on a terminal.

Synopsis terminal monitor

no terminal monitor

Operands None

Defaults The terminal monitor option is disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable the display of the RASlog and debug outputs on a terminal.

Usage Guidelines Use the **no terminal monitor** command to disable this option.

Examples To enable the display of the RASlog and the debug outputs on a terminal:

switch#terminal monitor

To disable the display of the RASlog and the debug outputs on a terminal:

switch#no terminal monitor

transmit-holdcount

Configures the maximum number of Bridge Protocol Data Units (BPDUs) transmitted per second for the Multiple Spanning Tree Protocol (MSTP) and the Rapid Spanning Tree Protocol (RSTP).

Synopsis transmit-holdcount number

no transmit-holdcount

Operands number Specifies the value in seconds for the number of BPDUs than can be sent

before pausing for 1 second. The range of valid values is from 1 through 10.

Defaults The default is 6.

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to configure the BPDU burst size by changing the transmit hold count value.

Use the no transmit-holdcount command to return to the default setting.

Usage Guidelines There are no usage guidelines for this command.

Examples To change the number of BPDUs transmitted to 3 seconds:

switch(conf-mstp)#transmit-holdcount 3

See Also show spanning-tree mst detail

unlock username

Unlocks a user who has been locked out due to unsuccessful login attempts.

Synopsis unlock username name

Operands name The name of the user.

Description Use this command to unlock a user who has been locked out.

Defaults There are no default configurations for this command.

Command Modes Privileged EXEC mode

Usage Guidelines There are no usage guidelines for this command.

Examples The following example unlocks a user:

switch# unlock username testUser

Result: Unlocking the user account is successful

See Also show running-config username, show users, username, unlock username

usb dir

Lists the contents of an attached USB device.

Synopsis usb dir [switchid switchID]

Operands switchid switchID Executes the command on a switch specified by its switch ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to list the contents of an attached USB device.

Usage Guidelines The USB device must be enabled before this function is available.

Examples To list the contents of the USB device attached to the local switch:

switch#usb dir

firmwarekey\ 0B 2010 Aug 15 15:13 support\ 106MB 2010 Aug 24 05:36 support1034\ 105MB 2010 Aug 23 06:11 config\ 0B 2010 Aug 15 15:13

firmware\ 380MB 2010 Aug 15 15:13 Available space on usbstorage 74%

See Also usb dir, usb off, usb on, usb remove

2 usb off

usb off

Disables an attached USB device.

Synopsis usb off [switchid switchID]

Operands switchid switchID Executes the command on a switch specified by its switch ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to disable an attached USB device. The device will be inaccessible until it is

enabled again.

Usage Guidelines A switch reload will automatically turn the USB device off.

Examples To disable a USB device attached to the local switch:

 $\verb|switch#usb| off \\$

USB storage disabled

See Also usb dir, usb on, usb remove

usb on

Enables an attached USB device.

Synopsis usb on [switchid switchID]

Operands switchid switchID Executes the command on a switch specified by its switch ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to enable an attached USB device.

Usage Guidelines The USB device must be enabled before the usb dir and usb remove commands are available.

Examples To enable a USB device attached to the local switch:

switch#usb on

USB storage enabled

See Also usb dir, usb off, usb remove

usb remove

Removes a file from an attached USB device.

Synopsis usb remove directory directory file file [switchid switchID]

Operands directory directory Specifies one the name of the directory where the file you want to remove is

located. Valid usb storage directories are firmware, firmwarekey, support,

and config.

file file Specifies the name of the file to be removed.

switchid switchID Executes the command on a switch specified by its switch ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to remove a directory or a file from an attached USB device.

Usage Guidelines The USB device must be enabled before this function is available.

Examples To remove a configuration file from a USB device attached to the local switch:

switch#usb remove directory config file startup-config.backup.

See Also usb dir, usb off, usb on

username

Assigns attributes for a username.

Synopsis username password password role role-name [desc description] [enable true | false]

no username name

Operands name Specifies the name of the user.

password The user's password.

password Specifies the user's password.

role The roles assigned to the user.

role-name Specifies the roles that are assigned to the user. The role is optional and, by

default, the user's role is read-only.

desc A description of the user.

description Specifies a description of the user. The text must be enclosed in double

quotes.

enable Whether a user is enabled or not.

default is true.

Description Use this command to assign attributes for a user.

Defaults The **enable** default is *true*.

The role default is read-only.

Command Modes Global configuration mode

Usage Guidelines Limit the username to 16 characters. The maximum number of user accounts on a switch is 64. The maximum number of roles for a user is 64, including the default roles.

Using the **no** form of the **username** command sets the default values of the individual attributes.

NOTE

All active login sessions for a user are terminated if the user's password or role is changed.

Examples The following example displays username attributes.

```
switch(config)# username testUser roles admin
Value for 'password' (<string>): *******
switch(config-username-testUser)# exit
switch(config)# username userBrocade password ******* role user desc "User to
monitor" enabled true
switch(config-username-userBrocade)#

switch# config
Entering configuration mode terminal
switch(config)# username testUser enabled false
switch(config-username-testUser) # desc "add op test user"
switch(config)# no username testUser desc
```

username

See Also show running-config username, show users, unlock username

VCS

Configures VCS parameters.

Synopsis vcs [rbridgeld ID] [vcsld ID] [enable rbridgeld]

no vcs enable

Operands rbridgeld ID Sets the RBridge ID for the switch. This parameter cannot be configured in

non-VCS mode unless the enabling operation is performed at the same time.

vcsld ID Sets the VCS ID. This parameter cannot be configured in non-VCS mode

unless the enabling operation is performed at the same time.

enable Enables VCS mode.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Use this command to configure the VCS parameters (VCS ID and the switch RBridge ID) and to enable VCS mode. You can set the VCS parameters and enable VCS mode at the same time, or you can enable VCS and then perform the ID assignments separately. Refer to the **Examples** section below for configuration possibilities.

Use the **no** form of this command to disable VCS mode.

Usage Guidelines

Description

Each time you change the VCS fabric configuration, the switch resets to the default configuration and reboots automatically. Make sure to save the configuration before you issue any of the following vcs commands.

- vcs enable
- no vcs enable
- vcs rbridgeld # enable
- vcs vcsld # enable
- vcs vcsID # rbridgeId # enable

Examples

Enable the VCS fabric by entering one of the following commands, based on your current configuration.

• If the VCS fabric is already disabled:

Command	Command Behavior
vcs enable	The RBridge ID is not changed, the VCS ID becomes 1, and VCS is enabled.
vcs vcsid x rbridgeId y enable	The RBridge ID is changed, the VCS ID is changed, and VCS is enabled.
vcs vcsid x enable	The RBridge ID is not changed, the VCS ID is changed, and VCS is enabled.
vcs rbridgeid y enable	The RBridge is changed, the VCS ID becomes 1, and VCS is enabled.

If the VCS fabric is already enabled:

vcs vcsid x rbridgeid y vcs vcsid x

no vcs enable

The VCS ID is changed and the RBridge ID is changed. Changes the VCS ID. $\,$

See Also show vcs

vepa enable

Activates the Virtual Ethernet Port Aggregator (VEPA) capability to U-turn traffic.

Synopsis vepa enable

no vepa enable

Operands None

Defaults Vepa capability is disabled.

Command Modes Interface configuration mode

Description This command activates the VEPA capability to U-turn the traffic on a single interface.

Usage Guidelines Use the **no vepa enable** command to disable the U-turn capability.

Examples switch(conf-te10/0/2)#vepa enable

virtual-fabric

Designates the Virtual Fabric Identification (VFID).

Synopis virtual-fabric 1

Operands None

Defaults There are no defaults for this command.

Command Modes FCoE fabric-map configuration mode

Description This command designates the VFID.

Usage Guidelines The VFID value is 1. No other values are allowed.

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Examples switch(config)#fcoe

switch(config-fcoe)#fabric-map default

switch(config-fcoe-fabric-map)#virtual-fabric 1

vlan classifier activate group

Activates a VLAN classifier group.

Synopsis vlan classifier activate group number vlan vlan_id

no vlan classifier activate group

Operands number Specifies which VLAN classifier group to activate. The range of valid values is

from 1 through 16.

vlan vlan_id Specifies which VLAN interface to activate. The range of valid values is from

1 through 3583.

Defaults There are no default configurations for this command.

Command Modes Interface configuration mode

Description Use this command to activate a VLAN classifier group for a specified VLAN. Use the **no vlan**

classifier activate group command to remove the specified group.

Usage Guidelines There are no usage guidelines for this command.

Examples To activate VLAN classifier group 1 for VLAN 5:

switch-cmsh(conf-if-te-0/10)#vlan classifier activate group 1 vlan 5

vlan classifier group

Adds and deletes rules to a VLAN classifier group.

Synopsis vlan classifier group number [add rule number] delete rule number]

Operands *number* Specifies the VLAN group number for which rules are to be added or deleted.

The range of valid values is from 1 through 16.

add rule number Specifies a rule is to be added. The range of valid values is from 1 through

256.

delete rule number Specifies a rule is to be deleted. The range of valid values is from 1 through

256.

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to add and delete rules from VLAN classifier groups.

Usage Guidelines Make sure your converged mode interface is not configured to classify untagged packets to the

same VLAN as the incoming VLAN-tagged packets. By configuring a converged interface to classify untagged packets (by using classifiers or the default port *vlan_id*) to the same VLAN as VLAN-tagged packets coming into the interface, the FCoE hardware sends out untagged packets to

the CNA. These packets may be dropped, disrupting communications.

Examples To add rule 1 to VLAN classifier group 1:

switch(config)#vlan classifier group 1 add rule 1

vlan classifier rule

Creates a VLAN classifier rule.

Synopsis vlan classifier rule rule_id [mac mac_address vlan vlan_id] [proto | arp | fcoe | fip | ip | ipv6]

[encap ethv2 | nosnaplic | snaplic]

no vian classifier rule rule_id

Operands rule_id Specifies the VLAN identification rule. The range of valid values is from 1

through 256.

mac Specifies the Media Access Control (MAC) list.

mac_address Specifies the MAC address-based VLAN classifier rule used to map to a

specific VLAN.

vian *vian_id* Specifies the VLAN. The range of valid values is from 1 through 65535.

proto Specifies the protocol to use for the VLAN classifier rule.

arp Specifies to use the Address Resolution Protocol.

fcoe Specifies to use the Fibre Channel over Ethernet Protocol.

fip Specifies to use the FCoE Initialization Protocol.

ip Specifies to use the Internet Protocol.

ipv6 Specifies to use the Internet Protocol version 6.

encap Specifies to encapsulate the Ethernet frames sent for the VLAN classifier

rule.

ethv2 Specifies to use the Ethernet version 2 encapsulated frames.

nosnaplic Specifies to use the Ethernet version 2 non-SNA frames.snaplic Specifies to use the Ethernet version 2 with SNA frames.

Defaults There are no default configurations for this command.

Command Modes Global configuration mode

Description Use this command to configure a VLAN classifier rule to dynamically classify Ethernet packets on

an untagged interface into VLANs. Use the **no vlan classifier rule** command to delete the VLAN

classifier rule specified by the rule_id.

Usage Guidelines VLAN classifiers can be created individually and can be managed separately. Up to 256 VLAN

classifiers can be provisioned. One or more VLAN classifiers can be grouped into a classifier group.

This classifier group can further be applied on an interface.

Examples To create an FCoE VLAN classifier rule:

switch(config)#vlan classifier rule 2 proto fcoe encap ethv2

See Also show vlan

vlan-profile (AMPP)

Activates the VLAN profile mode for AMPP.

Synopsis vlan-profile

Operands None

Defaults There are no defaults for this command.

Command Modes Port-profile mode

Description This command activates the VLAN profile mode for AMPP. This mode allows configuration of VLAN

attributes of a port-profile.

Usage Guidelines There are no usage guidelines for this command.

Examples Switch(config)#port-profile sample-profile

Switch(conf-pp)#vlan-profile