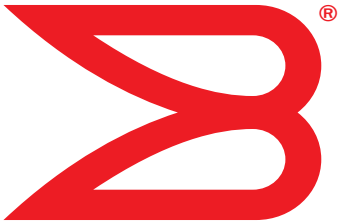
53-1002562-03
18 January 2013



Network OS

Command Reference

Supporting Network OS v3.0.0

BROCADE

Copyright © 2010-2012 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, MLX, NetIron, SAN Health, ServerIron, TurboIron, VCS, and VDX are registered trademarks, and AnyIO, Brocade One, CloudPlex, Effortless Networking, ICX, NET Health, OpenScript, and The Effortless Network are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks 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.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: 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

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 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
Network OS Command Reference	53-1002340-01	Updated for Network OS v2.1.0	September 2011
Network OS Command Reference	53-1002492-01	Updated for Network OS v2.1.1	December 2011
Network OS Command Reference	53-1002562-01	Updated for Network OS v3.0.0	September 2012
Network OS Command Reference	53-1002562-02	Updated for Network OS v3.0.0	October 2012
Network OS Command Reference	53-1002562-03	Updated for Network OS v3.0.0	January 2013

Contents

About This Document

How this document is organized xxiii
Supported hardware and software xxiii
What's new in this document xxiv
Document conventions xxiv
Text formatting xxiv
Command syntax conventions xxv
Notes, cautions, and warnings xxv
Key terms xxvi
Notice to the reader xxvi
Additional information xxvi
Brocade resources xxvi
Other industry resources xxvii
Getting technical help xxvii
Document feedback xxviii

Chapter 1 Using the Network OS CLI

DCB command line interface 1
Saving your configuration changes 1
Network OS CLI RBAC permissions 1
Default roles 1
Accessing the Network OS CLI through Telnet 2
Network OS CLI command modes 2
Network OS CLI keyboard shortcuts 5
Using the do command as a shortcut 5
Displaying Network OS CLI commands and command syntax . . 5
Network OS CLI command completion 7
Network OS CLI command output modifiers 7

Chapter 2 Network OS Commands

aaa accounting 9
aaa authentication 11
advertise dcbx-fcoe-app-tlv 12
advertise dcbx-fcoe-logical-link-tlv 13
advertise dcbx-iscsi-app-tlv 14
advertise dcbx-tlv 15
advertise dot1-tlv 16

advertise dot3-tlv 17
advertise optional-tlv 18
advertise-backup 19
advertisement interval (fabric-map) 20
advertisement-interval (VRRP) 21
allow non-profiled-macs. 22
area nssa 23
area range 24
area stub 25
area virtual-link 26
arp-ageing-timeout. 28
auto-cost reference-bandwidth 29
autoupload 30
banner login 31
bind 33
bpdu-drop enable. 34
bridge-priority 35
cee 36
cee-map (configuration) 37
cee-map (FCoE) 38
certutil import ldapca 39
certutil import syslogca 40
channel-group 41
chassis beacon 43
chassis disable. 44
chassis enable 45
chassis fan airflow-direction 46
cidrecov 47
cipherset. 50
cisco-interoperability 51
class 52
class-map 55
clear arp-cache 56
clear counters (IP) 57
clear counters (MAC) 59
clear counters access-list mac 61
clear counters storm-control 62

clear dot1x statistics 64
clear dot1x statistics interface 65
clear edge-loop-detection 66
clear fcoe login 67
clear ip igmp groups 68
clear ip igmp statistics 69
clear ip ospf 70
clear ip route 72
clear lacp 73
clear lacp counters 74
clear lldp neighbors 75
clear lldp statistics 76
clear logging auditlog 77
clear logging raslog 78
clear sflow statistics 79
clear spanning-tree counter 80
clear support 81
clear vrrp statistics 82
clock set 84
clock timezone 85
copy 86
copy default-config startup-config 88
copy running-config startup-config 89
copy support 90
copy support-interactive 91
database-overflow-interval 92
debug arp 93
debug ip 94
debug ip igmp 95
debug ip ospf 96
debug ip rtm 97
debug lacp 99
debug lldp packet 101
debug spanning-tree 102
debug vrrp 103
default-information-originate 105
default-metric 106

delete 107
deny (extended ACLs) 108
deny (standard ACLs) 110
description (interfaces) 111
description (LLDP) 112
description (Port Mirroring) 113
desire-distance 114
diag burninerrclear 115
diag clearerror 116
diag portledtest 117
diag portloopbacktest 119
diag post enable 121
diag prbstest 122
diag setcycle 124
diag systemverification 126
diag turboramtest 127
dir 129
distance 130
distribute-list route-map 131
dns 132
dot1x authentication 133
dot1x enable 134
dot1x port-control 135
dot1x quiet-period 136
dot1x reauthenticate interface 137
dot1x reauthentication 138
dot1x reauthMax 139
dot1x test eapol-capable 140
dot1x test timeout 141
dot1x timeout re-authperiod 142
dot1x timeout server-timeout 143
dot1x timeout supp-timeout 144
dot1x timeout tx-period 145
dpod 146
edge-loop-detection port-priority 147
edge-loop-detection VLAN 148
end 149

error-disable-timeout enable 150
error-disable-timeout interval 151
exit 152
external-lsdb-limit 153
fabric ecmp load-balance 154
fabric ecmp load-balance-hash-swap 155
fabric isl enable 156
fabric route mcast 157
fabric trunk enable 158
fabric vlag 159
fabric-map 160
fastboot 161
fcmap 162
fcoe 163
fcoe-profile (AMPP) 164
fcoeport 165
fcsp auth 166
fcsp auth-secret 168
fill-word 169
fips root disable 170
fips selftests 171
fips zeroize 172
firmware commit 173
firmware download 174
firmware restore 177
firmware sync 178
forward-delay 179
ha chassisreboot 181
ha disable 182
ha dump 183
ha enable 184
ha failover 185
hello 186
hello-interval 187
hello-time 188
hold-time 189
instance 190

interface 191
interface loopback 193
interface management 194
interface Ve 197
interface vlan 198
ip access-group 199
ip access-list 200
ip address 203
ip arp-aging-timeout 204
ip directed-broadcast 205
ip dns 206
ip igmp last-member-query-interval 207
ip igmp query-interval 208
ip igmp query-max-response-time 209
ip igmp snooping enable (global version) 210
ip igmp snooping enable 211
ip igmp snooping fast-leave 212
ip igmp snooping mrouter 213
ip igmp snooping mrouter-timeout 215
ip igmp snooping querier enable 216
ip igmp static-group 217
ip load-sharing 219
ip mtu 220
ip ospf area 221
ip ospf auth-change-wait-time 222
ip ospf authentication-key 223
ip ospf cost 224
ip ospf database-filter 225
ip ospf dead-interval 227
ip ospf hello-interval 228
ip ospf md5-authentication 229
ip ospf mtu-ignore 231
ip ospf network 232
ip ospf passive 233
ip ospf priority 234
ip ospf retransmit-interval 235
ip ospf transmit-delay 236

ip prefix-list 237
ip proxy-arp 238
ip route 239
ip route next-hop ospf 241
ip route next-hop-enable-default 242
ip route next-hop-recursion 243
ip router-id 244
ipv6 route 245
iscsi-priority 246
isl-r_rdy 247
keep-alive timeout (fabric-map) 248
l2traceroute 249
lacp port-priority 251
lacp system-priority 252
lacp timeout 253
ldap-server host 254
ldap-server maprole 255
license add 256
license remove 257
line vty exec-timeout 258
linecard 259
lldp dcbx-version 261
lldp disable 262
lldp iscsi-priority 263
lldp profile 264
logging auditlog class 265
logging raslog console 266
logging rbridge-id raslog console 267
logging syslog-facility local 268
logging syslog-server 269
long-distance 270
long-distance-isl 272
mac access-group 273
mac access-list extended 274
mac access-list standard 275
mac-address-reduction 276
mac-address-table 277

mac-rebalance 279
map 280
match interface 281
match ip address 282
match ip next-hop 283
match metric 284
match route-type 285
match tag 286
max-age 287
max-enodes 288
max-hops 289
max-metric router-lsa all-lsas 290
metric-type 291
minimum-links 292
mode 293
monitor session 294
multiplier 295
neighbor 296
no certutil ldapca 297
nssa-translator 298
ntp server 299
oscmd 300
password-attributes 302
pdu-rx-limit 304
permit (extended ACLs) 305
permit (standard ACLs) 307
ping 308
police-priority-map 310
policy-map 311
port-channel path-cost 312
port-profile 313
port-profile-port 314
power-off linecard 315
power-on linecard 316
precedence 317
preempt-mode 318
priority 319

priority-group-table 320
priority-tag 321
profile 322
prom-access disable 323
protect-mode enable 324
protocol edge-loop-detection 325
protocol lldp 326
protocol spanning-tree 327
pwd 328
qos cos 329
qos cos-mutation 330
qos cos-traffic-class 331
qos dscp-cos 332
qos dscp-mutation 333
qos dscp-traffic-class 334
qos flowcontrol tx 335
qos flowcontrol pfc 336
qos map cos-mutation 337
qos map cos-traffic-class 338
qos map dscp-cos 339
qos map dscp-mutation 340
qos map dscp-traffic-class 342
qos red profile 343
qos trust cos 344
qos trust dscp 345
qos queue multicast scheduler 346
qos queue scheduler 348
qos rcv-queue cos-threshold 350
qos random-detect cos 352
qos rcv-queue multicast rate-limit 353
qos rcv-queue multicast threshold 354
qos-profile (AMPP) 356
radius-server 357
rate-limit-delay get netconf 359
rate-limit-delay set netconf 360
redistribute 361
region 362

reload 363
remap fabric-priority 364
remap lossless-priority. 365
rename 366
resequence. 367
reserved-vlan 368
revision 369
rfc1583-compatibility 370
rfc1587-compatibility 371
rmon alarm. 372
rmon collection history 373
rmon collection stats 374
rmon event 375
role 376
route-map 377
router ospf 378
rule 379
secpolicy activate. 380
secpolicy defined-policy. 381
security-profile (AMPP) 383
seq (extended IP ACLs) 384
seq (standard IP ACLs). 387
seq (extended MAC ACLs) 389
seq (standard MAC ACLs) 391
service password-encryption. 392
service-policy 393
set distance 394
set ip next-hop 395
set metric 396
set tag. 397
sflow collector 398
sflow enable (global version). 399
sflow enable (interface version) 400
sflow polling-interval (global version) 401
sflow polling-interval (interface version). 402
sflow sample-rate (global version) 403
sflow sample-rate (interface version) 404

short-path-forwarding 405
show access-list 406
show access-list interface 407
show arp 408
show autoupload 410
show calendar 411
show cee maps 412
show cert-util ldapca 413
show chassis 414
show cipherset 418
show clock 419
show copy-support status 420
show debug ip igmp 421
show debug lacp 422
show debug lldp 423
show debug spanning-tree 424
show debug vrrp 425
show default-vlan 426
show diag burninerrshow 427
show diag burninerrshowerrLog 428
show diag burninstatus 430
show diag post results 431
show diag setcycle 433
show diag status 434
show dot1x 435
show dot1x all 436
show dot1x diagnostics interface 437
show dot1x interface 438
show dot1x session-info interface 439
show dot1x statistics interface 440
show dpod 441
show edge-loop-detection globals 442
show edge-loop-detection interface 443
show edge-loop-detection rbridge-id 444
show environment fan 445
show environment history 447
show environment power 449

show environment sensor 450
show environment temp 451
show fabric all 452
show fabric ecmp load-balance 453
show fabric isl. 454
show fabric islports 456
show fabric route linkinfo 459
show fabric route multicast. 461
show fabric route neighbor-state 463
show fabric route pathinfo. 465
show fabric route topology 473
show fabric trunk 475
show fabric vlag-load-balance. 477
show fcoe fabric-map 478
show fcoe interface 479
show fcoe login 480
show fcoe map. 481
show fcsp auth-secret dh-chap. 482
show file 483
show fips. 484
show firmwaredownloadhistory 485
show firmwaredownloadstatus. 486
show ha 487
show interface 489
show interface FibreChannel 492
show interface management 498
show ip fib 500
show ip igmp groups 501
show ip igmp interface vlan 503
show ip igmp snooping 504
show ip igmp statistics interface 505
show ip interface 506
show ip ospf 508
show ip ospf area. 509
show ip ospf border-routers. 511
show ip ospf config 512
show ip ospf database. 514

show ip ospf interface 517
show ip ospf neighbor 519
show ip ospf routes 521
show ip ospf summary 522
show ip ospf traffic 523
show ip ospf virtual 525
show ip route 526
show lacp counters 529
show lacp sys-id 530
show license 531
show license id 532
show linecard 533
show lldp interface 535
show lldp neighbors 536
show lldp statistics 538
show logging auditlog 539
show logging raslog 540
show mac-address-table 542
show media 544
show media interface 545
show media linecard 548
show mm 550
show monitor 551
show name-server brief 552
show name-server detail 553
show name-server nodefind 555
show name-server zonemember 556
show netconf client-capabilities 558
show netconf-state capabilities 559
show netconf-state datastores 560
show netconf-state schemas 561
show netconf-state sessions 562
show netconf-state statistics 563
show ntp status 564
show policymap 565
show port port-channel 567
show port-channel 568

show port-profile 569
show port-profile interface 570
show port-profile name 571
show port-profile status 572
show process cpu 573
show process info 574
show process memory 575
show prom-access 576
show qos flowcontrol interface 577
show qos interface 579
show qos maps 581
show qos maps dscp-cos 582
show qos maps dscp-mutation 583
show qos maps dscp-traffic-class 584
show qos queue interface 585
show qos rcv-queue interface 586
show qos rcv-queue multicast 587
show qos red profiles 588
show qos red statistics interface 590
show rmon 591
show rmon history 593
show running reserved-vlan 594
show running-config 595
show running-config aaa 596
show running-config aaa accounting 597
show running-config access-list ip 598
show running-config access-list mac 599
show running-config banner 600
show running-config cee-map 601
show running-config class-map 602
show running-config diag post 603
show running-config dot1x 604
show running-config dpod 605
show running-config fabric route mcast 606
show running-config fcoe 607
show running-config fcsp auth 608
show running-config interface fcoe 609

show running-config interface FibreChannel 610
show running-config interface gigabitethernet 612
show running-config interface gigabitethernet bpdu-drop . . .613
show running-config interface
gigabitethernet channel-group 614
show running-config interface gigabitethernet description . .615
show running-config interface gigabitethernet dot1x 616
show running-config interface gigabitethernet lacp 618
show running-config interface gigabitethernet lldp. 619
show running-config interface gigabitethernet mac 620
show running-config interface gigabitethernet mtu 621
show running-config interface
gigabitethernet port-profile-port 622
show running-config interface gigabitethernet priority-tag . . .623
show running-config interface gigabitethernet qos. 624
show running-config interface gigabitethernet rmon 625
show running-config interface gigabitethernet sflow 626
show running-config interface gigabitethernet shutdown. . . .627
show running-config interface gigabitethernet switchport . . .628
show running-config interface gigabitethernet vlan 629
show running-config interface management. 630
show running-config interface port-channel 631
show running-config interface tengigabitethernet. 632
show running-config interface
tengigabitethernet bpdu-drop 633
show running-config interface tengigabitethernet cee 634
show running-config interface
tengigabitethernet channel-group 635
show running-config interface
tengigabitethernet description 636
show running-config interface tengigabitethernet dot1x 637
show running-config interface tengigabitethernet fabric 639
show running-config interface tengigabitethernet fcoeport . .640
show running-config interface tengigabitethernet lacp. 641
show running-config interface tengigabitethernet lldp 642
show running-config interface tengigabitethernet mac 643
show running-config interface tengigabitethernet mtu. 644
show running-config interface
tengigabitethernet port-profile-port 645

show running-config interface tengigabitethernet priority-tag. 646
show running-config interface tengigabitethernet qos 647
show running-config interface tengigabitethernet rmon. 648
show running-config interface tengigabitethernet sflow. 649
show running-config interface tengigabitethernet shutdown 650
show running-config interface tengigabitethernet switchport. 651
show running-config interface tengigabitethernet vlan. 652
show running-config interface vlan. 653
show running-config interface vlan ip. 654
show running-config ip access-list 656
show running-config ip dns 657
show running-config ip igmp 658
show running-config ip route. 659
show running-config ldap-server. 660
show running-config line 661
show running-config logging 662
show running-config logging auditlog class 663
show running-config logging raslog 664
show running-config logging syslog-facility. 665
show running-config logging syslog-server. 666
show running-config monitor. 667
show running-config ntp 668
show running-config password-attributes 669
show running-config police-priority-map. 670
show running-config policy-map 671
show running-config port-profile. 672
show running-config port-profile activate. 673
show running-config port-profile fcoe-profile 674
show running-config port-profile qos-profile 675
show running-config port-profile security-profile 676
show running-config port-profile static. 677
show running-config port-profile vlan-profile 678
show running-configuration protocol cdp. 680
show running-configuration protocol edge. 681
show running-configuration protocol lldp. 682

show running-config radius-server 683
show running-config rbridge-id 684
show running-config rbridge-id linecard 685
show running-config rmon 686
show running-config role 687
show running-config rule 688
show running-config secpolicy 690
show running-config ssh server 691
show running-config snmp-server 692
show running-config support 694
show running-config switch-attributes 695
show running-config system-monitor 696
show running-config system-monitor-mail 697
show running-config tacacs-server 698
show running-config telnet server 699
show running-config threshold-monitor 700
show running-config threshold-monitor interface 701
show running-config threshold-monitor security 702
show running-config threshold-monitor sfp 703
show running-config username 704
show running-config zoning 705
show running-config zoning defined-configuration 707
show running-config zoning enabled-configuration 709
show secpolicy 711
show sflow 712
show sfm 713
show slots 715
show spanning-tree 717
show spanning-tree brief 719
show spanning-tree interface 720
show spanning-tree mst brief 722
show spanning-tree mst detail 723
show spanning-tree mst instance 726
show spanning-tree mst interface 727
show ssh server status 729
show startup-config 730
show startup-db 731

show statistics access-list 732
show statistics access-list interface 733
show storm-control 734
show support 736
show system 737
show system monitor 738
show telnet server status 739
show users 740
show vcs 741
show version 743
show vlan 745
show vlan classifier 746
show vnetwork 747
show vrrp 750
show zoning operation-info 752
shutdown 753
shutdown (STP) 754
shutdown-time 755
snmp-server 756
snmp-server community 759
snmp-server contact 760
snmp-server location 761
snmp-server sys-descr 762
snmp-server user 763
snmp-server v3host 765
source 766
spanning-tree autoedge 768
spanning-tree bpdu-mac 769
spanning-tree cost 770
spanning-tree edgeport 771
spanning-tree guard root 772
spanning-tree hello-time 773
spanning-tree instance 774
spanning-tree link-type 775
spanning-tree portfast 776
spanning-tree priority 777
spanning-tree restricted-role 778

spanning-tree restricted-tcn 779
spanning-tree shutdown 780
speed (Ethernet) 781
speed (Fibre Channel) 782
speed (Port-channel) 783
speed (LAG) 784
ssh. 785
ssh server shutdown 787
storm-control ingress 788
summary-address 790
support 791
switch-attributes. 792
switchport. 794
switchport access 795
switchport mode 796
switchport trunk allowed vlan 797
switchport trunk native-vlan 798
switchport trunk tag native-vlan 799
system-description. 800
system-monitor. 801
system-monitor-mail 804
system-name 806
tacacs-server 807
telnet. 809
telnet server shutdown 810
terminal 811
threshold-monitor cpu 812
threshold-monitor interface 814
threshold-monitor memory 818
threshold-monitor security 820
threshold-monitor sfp 822
timers 825
traceroute 826
track 827
transmit-holdcount. 829
trunk-enable 830
unhide fips 831

unlock username 832
usb 833
usb dir 834
usb remove 835
username 836
vc-link-init 838
vcenter 839
vcs 840
vcs virtual ip 842
virtual-fabric 843
virtual-ip 844
vlag ignore-split 845
vlan classifier activate group 846
vlan classifier group 847
vlan classifier rule 848
vlan dot1q tag native 849
vlan-profile (AMPP) 850
vnetwork vcenter MYVC discover 851
vrrp-extended-group 852
vrrp-group 853
zoning defined-configuration alias 854
zoning defined-configuration cfg 856
zoning defined-configuration zone 858
zoning enabled-configuration cfg-action cfg-clear 860
zoning enabled-configuration cfg-action cfg-none 861
zoning enabled-configuration cfg-action cfg-save 862
zoning enabled-configuration cfg-action cfg-transaction-abort863
zoning enabled-configuration cfg-name 864
zoning enabled-configuration default-zone-access 865

About This Document

In this chapter

- How this document is organized xxiii
- Supported hardware and software. xxiii
- What's new in this document xxiv
- Document conventions xxiv
- Notice to the reader xxvi
- Additional information xxvi
- Getting technical help xxvii
- Document feedback xxviii

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 3.0.0, 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:

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

- Brocade VDX 6710-54
- Brocade VDX 6720
  - Brocade VDX 6720-24
  - Brocade VDX 6720-60
- Brocade VDX 6730
  - Brocade VDX 6730-32
  - Brocade VDX 6730-76
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8

To obtain information about an OS version other than Network OS v3.0.0, refer to the documentation specific to that OS version.

What's new in this document

- This version has been updated to support Network OS v3.0.0.
- Revised description for the "chassis fan airflow-direction" command on page 46.

For complete information, refer to the Release Notes.

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
`code` text	Identifies CLI output 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	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 Brocade VCS Fabric technology® 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 xxvi 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.

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 on the switch ID pull-out tab located on the bottom of the port side of the switch.
3. World Wide Name (WWN)

   Use the **show license id** command to display the WWN of the chassis.

   If you cannot use the **show license id** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

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.

Chapter

1

Using the Network OS CLI

In this chapter

- DCB command line interface 1

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 *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 v3.0.0 supports up to 32 Telnet sessions with the admin login.

Network OS CLI command modes

Table 1 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 1 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)#`
	
	VLAN:
	`switch(conf-Vlan-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.

TABLE 1 Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description

Protocol configuration	LLDP:
	`switch(conf-lldp)#`
	
	Spanning-tree:
	`switch(conf-mstp)#`
	`switch(conf-rstp)#`
	`switch(conf-stp)#`
	`switch(conf-pvst)#`
	`switch(conf-rpvst)#`
		From the global configuration mode, specify a protocol by entering one of the following commands:
		• **protocol lldp**
		• **protocol spanning-tree mstp**
		• **protocol spanning-tree rstp**
		• **protocol spanning-tree stp**
		• **protocol spanning-tree pvst**
		• **protocol spanning-tree rapid-pvst**
			Access and configure protocols.

FCoE configuration	FCoE:
	`switch(config-fcoe)#`
	
	FCoE fabric-map sub-mode:
	`switch(config-fcoe-fabric-map)#`
	
	FCoE map sub-mode:
	`switch(config-fcoe-map)#`
		From the global configuration mode, use the **fcoe** command to enter FCoE configuration mode.
		
		From the FCoE configuration mode, specify an FCoE sub-mode by entering one of the following commands:
		• **fabric-map default**
		• **map default**
			Access and configure FCoE features.

AMPP port-profile mode	AMPP port-profile:
	`switch(conf-port-profile-name)#`
	
	VLAN-profile sub-mode:
	`switch(conf-vlan-profile)#`
	
	QoS-profile sub-mode:
	`switch(conf-qos-profile)#`
	
	FCoE-profile sub-mode:
	`switch(conf-fcoe-profile)#`
	
	Security-profile sub-mode:
	`switch(conf-security-profile)#`
		From the global configuration mode, enter the **port-profile** command to enter port-profile configuration mode.
		
		From the port-profile configuration mode, specify an AMPP sub-mode by entering one of the following commands:
		• **vlan-profile**
		• **qos-profile**
		• **fcoe-profile**
		• **security-profile**
			Access and configure AMPP features.

Feature configuration	CEE map:
	`switch(config-cee-map-default)#`
	
	Standard ACL:
	`switch(conf-macl-std)#`
	
	Extended ACL:
	`switch(conf-macl-ext)#`
		From the global configuration mode, specify a DCB feature by entering one of the following commands:
		• **cee-map default**
		• **mac access-list standard**
		• **mac access-list extended**
			Access and configure CEE map features.

DSCP mutation mapping	DSCP Mutation Map: `switch(dscp-mutation-mapname)#`	From the global configuration mode, remap incoming DSCP values using the following command: **qos map dscp-mutation** map*name*	

TABLE 1 Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description
DSCP to CoS priority mapping	DSCP to CoS Map: `switch(dscp-cos-mapname)#`	From the global configuration mode, create a DSCP to CoS priority map using the following command: **qos map dscp-cos** map*name*	
DSCP to traffic class mapping	DSCP to Traffic Class Map: `switch(dscp-traffic-class-mapnam e)#`	From the global configuration mode, create a DSCP to traffic class map using the following command: **qos map dscp-traffic-class** map*name*	
DSCP to traffic class mapping	DSCP to Traffic Class Map: `switch(dscp-traffic-class-mapnam e)#`	From the global configuration mode, create a DSCP to traffic class map using the following command: **qos map dscp-traffic-class** map*name*	
QoS Policer configuration	Police Priority Map `switch(config-policemap)#` Class Map: switch(config-classmap) Policy Map: switch(config-policymap) Policy-class-map submode switch(config-policymap-class) Policy-class-map-policer attributes submode switch(config-policymap-class-police)	From the global configuration mode, specify a Policer configuration mode by entering one of these command: • **police-priority-map** *mapname* • **class-map** *mapname* • **policy-map** *mapname* To enter the pollicy-class-map sub-mode from the policy-map mode, enter **class** *classmap name* To enter the policy-class-map-policer attributes sub-mode from the policy-map-class mode, enter **police** followed by policing attributes.	

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 2 lists Network OS CLI keyboard shortcuts.

TABLE 2 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.

```
switch(conf-lldp)#do dir
Contents of flash://
   -rw-r-----            1276   Wed Feb  4 07:08:49 2009    startup_rmon_config
   -rw-r-----            1276   Wed Feb  4 07:10:30 2009    rmon_config
   -rw-r-----            1276   Wed Feb  4 07:12:33 2009    rmon_configuration
   -rw-r-----            1276   Wed Feb  4 10:48:59 2009    starup-config
```

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.

```
switch(conf-lldp)# ?
Possible completions:
  advertise           The Advertise TLV configuration.
  description         The User description
  disable             Disable LLDP
```

```
  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
  mode                The LLDP mode.
  multiplier          The Timeout Multiplier
  no                  Negate a command or set its defaults
  profile             The LLDP Profile table.
  pwd                 Display current mode path
  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 (**?**).

```
switch#terminal ?
Possible completions:
  length    Sets Terminal Length for this session
  monitor   Enables terminal monitoring for this session
  no        Sets Terminal Length for this session to default :24.
  timeout   Sets the interval that the EXEC command interpreter wait for user
            input.
```

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.

```
switch#show i?
  interface  Interface status and configuration
  ip         Internet Protocol (IP)
```

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.

```
switch#hookup
        ^
syntax error: unknown argument.
```

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

```
switch#show
          ^
syntax error: unknown argument.
```

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 l** and press **Tab**:

```
switch#show l
```

The CLI displays the following command.

```
switch#show l
Possible completions:
  lacp
  license   Display license keys installed on the switch.
  lldp      Link Layer Discovery Protocol(LLDP).
  logging   Show logging
```

Network OS CLI command output modifiers

You can filter the output of the CEE CLI **show** commands using the output modifiers described in Table 3.

TABLE 3 CEE CLI command output modifiers

Output modifier	Description
append	Appends the output to a file.
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.
until *string*	Ends the output when the output text matches the string.
count	Counts the number of lines in the output.
linnum	Enumerates the lines in the output.

TABLE 3 CEE CLI command output modifiers (Continued)

Output modifier	Description
more	Paginates the output.
nomore	Suppresses the pagination of the output.
FLASH	Redirects the output to flash memory.

Chapter

Network OS Commands

2

aaa accounting

Enables or disables the TACACS+ accounting service.

Synopsis **aaa accounting exec default start-stop tacacs+** [**none**]

[**no**] **aaa accounting exec default start-stop tacacs+**

aaa accounting commands default start-stop tacacs+

[**no**] **aaa accounting commands default start-stop tacacs+** [**none**]

Operands

exec	Enables login accounting.
commands	Enables command accounting.
default	Specifies the default mode.
start-stop	Sends start-stop packet upon completion of a command or login.
none	Disables accounting. This operand is optional and functionally equivalent to the **no** version of the command.
tacacs+	Uses the TACACS+ server for accounting.

Defaults AAA accounting is disabled by default.

Command Modes Global configuration mode

Description Use this command to enables or disables the TACACS+ protocol-based accounting service.

When login accounting is enabled, all logins will be logged. An accounting stop packet will be sent with relevant attributes to the TACACS+ server when the login is terminated.

When command accounting is enabled, an accounting stop packet will be sent with relevant attributes to the TACACS+ server once the command execution is completed. Most configuration commands, non-configuration commands such as show commands, or operations such as firmware download are logged..For a listing of commands that are not accounted for, refer to the *Network OS Administrator's Guide,* Appendix A, "TACACS+ Accounting Exceptions"

Usage Guidelines Login or command accounting can be enabled only if at least one TACACS+ server host is configured. Similarly, if either login or command accounting is enabled, you cannot remove the TACACS+ server can't be removed if it is the only server available.

The **no aaa accounting exec default start-stop tacacs+** disables login accounting.

The **no aaa accounting command default start-stop tacacs+** disables command accounting. You can also use the optional "none" operand to disable accounting.

Examples To enable command accounting:

```
switch(config)# accounting command default start-stop tacacs+
```

To enable login accounting:

```
switch(config)# accounting command default start-stop tacacs+
```

To disable command accounting using the “no” operand:

```
switch(config)# no accounting command default start-stop tacacs+
```

To disable command accounting using the “none” operand:

```
switch(config)# accounting command default start-stop none
```

See Also show running-config tacacs-server, tacacs-server

aaa authentication

Configures the AAA login sequence.

Synopsis **aaa authentication login** {**default** | **ldap** | **local** | **radius** | **tacacs+**} [**local**]

no aaa authentication login

Operands

login		Specifies the type of server that will be used for authentication, authorization, and accounting (AAA) on the switch. The local server is the default. Specify one of the following options:
	default	Specifies the default mode (Local server). Authenticates the user against the local database only. If the password does not match or the user is not defined, the login fails.
	ldap	Specifies the Lightweight Directory Access Protocol (LDAP) servers.
	local	Specifies the local switch database.
	radius	Specifies the RADIUS servers.
	tacacs+	Specifies the TACACS+ servers.
	[**local**]	Specifies the local switch database with any of the AAA server options.

Default The default server is local.

Command Modes Global configuration mode

Description Use this command to select the order of authentication sources to be used for user authentication during the login process. Two sources are supported: primary and secondary. The secondary source of authentication is optional and will be used if the primary source fails or is not available.

Usage Guidelines The authentication mode can only be set and cannot be added or deleted. For example, to change a configuration from “radius local” to radius only, execute the **no aaa authentication login** command to resets the configuration to the default mode, and then reconfigure the AAA mode with the desired setting.

Examples To change the AAA server to TACACS+ using the local switch database as a secondary source of authentication:

```
switch(config)# aaa authentication login tacacs+ local
Broadcast message from root (pts/0) Tue Apr  5 16:34:12 2011...

AAA Server Configuration Change: all accounts will be logged out
```

To change the AAA server from TACACS+ and local to TACACS+ only (no secondary source):

```
switch(config)# no aaa authentication login tacacs+ local
switch(config)# aaa authentication login tacacs+
switch(config)# do show running-config aaa
aaa authentication login tacacs+
```

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 None

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.

Usage Guidelines 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**

advertise dcbx-iscsi-app-tlv

Advertises the iSCSI traffic configuration parameters for TLV.

Synopsis **advertise dcbx-iscsi-app-tlv**

no advertise dcbx-iscsi-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.

Usage Guidelines Use the **no advertise dcbx-iscsi-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 None

Examples None

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

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 None

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 None

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 advertise the following optional TLVs.

Usage Guidelines Use the **no advertise optional-tlv** command to return to the default setting.

Examples None

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

advertise-backup

Enables a backup router to send advertisement frames to the master router.

Synopsis **advertise-backup**

no advertise backup

Operands There are no operands for this command.

Default Disabled by default.

Command Modes Virtual-router-group configuration mode.

Description Enables a backup router to send periodic transmissions of advertisement frames to all routers in the network. If a backup router is enabled to send advertisement frames, the frames are sent every 60 seconds by default.

Usage Guidelines This command can be used for VRRP-E but not for VRRP. Use the **no** parameter with this command to stop the periodic transmission.

Examples To enable the backup routers in a specific virtual router to send advertisement frames to the master router:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-Ve-25)# vrrp-extended-group 1
switch(config-vrrp-extended-group-1)# advertise-backup
```

See Also vrrp-group

advertisement interval (fabric-map)

Configures the FIP 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 90000 milliseconds.

Defaults The default value is 8000 milliseconds.

Command Modes FCoE fabric-map configuration mode

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

Usage Guidelines 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**

advertisement-interval (VRRP)

Configures the interval at which the master advertises its existence to the backup routers.

Synopsis **advertisement-interval** *range*

Operands

range	Interval, in seconds, at which the master advertises its existence to the backup routers. Range: 1-255

Default The default for *range* is one second.

Command Modes Virtual-router-group configuration mode.

Description Configures the advertisement interval of the virtual router. This interval is the length of time, in seconds, between each advertisement sent from the master to its backup physical routers. The advertisement notifies the backup routers that the master is still active. If the backup routers do not receive an advertisement from the master in a designated amount of time, the backup with the highest priority can assume the role of master.

Usage Guidelines This command can be used for either VRRP or VRRP-E.

Examples To set the advertisement interval to 30 seconds for VRRP-E group 10:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-Ve-25)# vrrp-extended-group 10
switch(config-vrrp-extended-group-10)# advertisement-interval 30
```

See Also **vrrp-group**

allow non-profiled-macs

Specifies whether non-profiled macs on the profiled port are dropped.

Synopsis **allow non-profiled-macs**

no allow non-profiled-macs

Operands None

Defaults None

Command Modes Port-profile mode

Description This command allows you to decide whether non-profiled macs on profiled port should be dropped or not. This configuration is allowed on the default profile only.

Usage Guidelines Use the **no allow non-profiled-macs** command to disable this functionality.

Examples To allow non-profiled macs:

```
switch(config)# port-profile default
switch(config-port-profile-default)# allow non-profiled-macs
```

See Also None

area nssa

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Synopsis **area** {*A.B.C.D* | *decimal*} **nssa** {*metric* [**no-summary**] | **default-information-originate**}

Operands

A.B.C.D	Area address in dotted decimal format.
decimal	Area address In decimal Format.
metric	Additional cost for using a route to or from this area.
no-summary	When configured on the NSSA area border router (ABR), this option prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA an NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs. This option is disabled by default, which means the default route must use a Type 7 LSA.
default-information-originate	When configured on the ABR, this option injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. The NSSA ABR does not, by default, originate a default route to the NSSA.

Default None—No areas are created by default.

Command Modes Router configuration mode.

Description Creates an NSSA area or modifies its parameters. NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

Usage Guidelines Use the **no** parameter to delete an NSSA.

Examples To set an additional cost of 5 on an NSAA called 2 (in decimal format), and include the no-summary option:

```
Switch(conf-ospf-router)# area 2 nssa 5 no-summary
```

area range

Specifies area range parameters on an Area Border Router (ABR).

Synopsis **area** {*A.B.C.D* | *decimal*} **range** *E.F.G.H I.J.K.L* {**advertise** | **not-advertise**}

Operands

A.B.C.D	Area address in dotted decimal format.
decimal	Area address in decimal format.
E.F.G.H I.J.K.L	Specifies the IP address and mask portion of the range. All network addresses that match this network are summarized in a single route and advertised by the ABR.
advertise	Sets the address range status to *advertise* and generates a Type 3 summary LSA.
not-advertise	Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Default None.

Command Modes Router configuration mode.

Description This command is used only on ABRs to specify route summarization for an existing area. The result is that a single summary route is advertised to other areas by the ABR, in the form of a Type 3 LSA. Routing information is condensed at area boundaries and external to the area, and only a single route is advertised for each address range.

An example of when you might want to use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summarization is allowed within the area.

Usage Guidelines Use the **no** parameter to disable the specification of range parameters on an ABR.

Examples To advertise to Area 3 all the addresses on the network 1.1.1.0 255.255.255.0 in the ABR you are signed into:

```
Switch(conf-ospf-router)# area 3 range 1.1.1.0 255.255.255.0 advertise
```

area stub

Creates a stub area or modifies its parameters.

Synopsis **area** {*A.B.C.D* | *decimal*} **stub** *metric* **[no-summary]**

Operands

A.B.C.D	Area address in dotted decimal format.
decimal	Area address In decimal Format.
metric	Additional cost for using a route to or from this area.
no-summary	When configured on the ABR, prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a default route is injected into the stub/totally stubby area by the ABR as a Type 3 LSA. Enabling this option makes the area a so-called totally stubby area, which can only have Types 1 and 2. This option is disabled by default.

Default None—No areas are created by default.

Command Modes Router configuration mode.

Description Creates or deletes a stub area or modifies its parameters.

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

Usage Guidelines Use the **no** parameter to delete a stub area.

Examples To set an additional cost of jj5 on a stub area called 2 (in decimal format):

```
Switch(conf-ospf-router)# area 2 stub 5
```

area virtual-link

Creates or modifies virtual links for an area.

Synopsis **area** {*A.B.C.D* | *decimal*} **virtual-link** *E.F.G.H* [**authentication-key** {**0** | **2** | **255**} *password*] [**dead-interval** *time*] [**hello-interval** *time*] [**md5-authentication** {**key-activation-wait-time** *time* | **key-id** *num key*}] [**retransmit-interval** *time*] [**transmit-delay** *time*]

Operands

A.B.C.D	Area address in dotted decimal format.
decimal	Area address in decimal format.
E.F.G.H	ID of the OSPF router at the remote end of the virtual link.
authentication-key	Sets password and encryption method. Only one encryption method can be active on an interface at a time. All OSPF packets transmitted on the interface contain this password. All OSPF packets received on the interface are checked for this password. If the password is not present, then the packet is dropped.
0	Does not encrypt the password you enter.
2	Encrypts the password you enter.
255	Encrypts a plain-text password that you enter.
password	OSPF password. The password can be up to eight alphanumeric characters.
dead-interval *time*	The number of seconds that a neighbor router waits for a hello packet from the current router before declaring the router down. This value must be the same for all routers and access servers that are attached to a common network. The default is 40. The range is 3 to 65535.
hello-interval	Time (in seconds) between hello packets that the router sends on an interface. The value must be the same for all routers and access servers that are attached to a common network. The default is 10 seconds. The range is 1 to 65535.
md5-authentication	Sets either MD5 key-activation wait time or key identifier.
key-activation-wait-time *time*	Time in seconds before a newly configured MD5 authentication key is valid. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. The default value is 300. The range is 0 to 14400.
key-id *num key*	The *num* is a number from 1 – 255 and identifies the MD5 key that is being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the *key* is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.

retransmit-interval *time*
Time (in seconds) between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two routers on the attached network. The default is 5. The range is 0 to 3600.

transmit-delay *time*
Estimated time (in seconds) required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet gets incremented by the value of this operand before transmission occurs. The default value is 1. The range is 0 to 3600.

Default None—No virtual links are created by default.

Command Modes Router configuration mode.

Description Creates or modifies virtual links for an area.

Usage Guidelines Use the **no** parameter to remove a virtual link.

Examples To create a virtual link for an area whose decimal address is 1, and where the ID of the OSPF router at the remote end of the virtual link is 10.1.2.3:

```
switch(conf-ospf-router)# area 1 virtual-link 10.1.2.3
```

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. The range of valid values is from 0 through 35790 minutes.

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.

This command does not function in VCS mode.

Examples None

See Also None

auto-cost reference-bandwidth

Configures reference bandwidth.

Synopsis **auto-cost reference-bandwidth** {*ref-bw* | **use-active-ports**}

Operands

ref-bw	Reference bandwidth in Mbps. The reference bandwidth range is 1 to 4294967.
use-active-ports	When set, any dynamic change in bandwidth immediately affects the cost of OSPF routes. This option enables cost calculation for currently active ports only.

Default The default reference bandwidth is 100 Mbps.

Command Modes Router configuration mode

Description Configures the reference bandwidth. OSPF calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

Usage Guidelines The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group – The combined bandwidth of all the ports.
- Virtual interface – The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

NOTE
If you specify the cost for an individual interface (by using the **ip ospf cost** command), the cost you specify overrides the cost calculated by the software.

You can use the **no** parameter with this command to disable bandwidth configuration.

Examples To change a reference bandwidth of 500:

```
switch(config)# router ospf
switch(conf-ospf-router)# auto-cost reference-bandwidth 500
```

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.

The costs for 10 Mbps and 100 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

See Also **ip ospf cost**

autoupload

Enables or disables autoupload of FFDC and trace support data.

Synopsis **autoupload {enable | disable} host** *ip_address* **user** *user_name* **directory** *dir* **[rbridge-id** *rbridge-id***] password** *password*

Operands

enable	Enables the autoupload feature.
host *host_ip*	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
user *username*	Specifies the user login name for the server.
directory *dir*	Specifies a fully qualified path to the directory **where the data will be stored.**
rbridge-id *rbridge-id*	Executes the command on a remote RBridge specified by the ID of the routing bridge. This option is not valid in standalone mode and currently not supported.
password *password*	Specifies the account password.
disable	Disables the autoupload feature.

Defaults Autoupload is disabled by default.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable autoupload of FFDC and trace data files to the remote location configured for saving support data.

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

If you re-enable autoupload after it was disabled, you must reissue the command with all required parameters.

Examples To enable autoupload for a specified host:

```
switch# autoupload enable host 10.31.2.27 directory
/users/support/ffdc_autoupload user supportadmin password *******
Support auto file transfer enabled.
```

To disable autoupload:

```
switch# autoupload disable
Support auto file transfer disabled.
```

See Also **show autoupload**

banner login

Sets the switch banner.

Synopsis **banner login** *message*

no banner login

Operands *message* The message string to be displayed on the switch console.

Defaults None

Command Modes Global configuration mode

Description Use this command to create a switch banner. A banner is a text message that displays on the console. The banner can include information about the switch that a user wants another user to know when accessing the switch.

Usage Guidelines The banner must be from 1 through 1022 characters in length.

The banner can appear on multiple lines if you enter multiline mode using ESC-M and using CTRL-D to exit.

Examples To create a banner with multiple lines:

```
switch(config)# banner login [Esc-m]
[Entering multiline mode, exit with ctrl-D.]
> banner login Hello
> and
> welcome
> to
> the
> switch
[Ctrl-D]
switch(config)# do show running-config banner
banner login "Hello\and\welcome\to\the\switch"
switch(config)# exit

Network OS (switch)
NOS Version 3.0.0


switch login: admin
Password: ******

Hello
and
welcome
to
the
switch
```

To create a banner with a single line:

```
switch(config)# banner login “Please do not disturb the setup on this switch”
switch(config)# exit

Login: user
```

```
Password: *****

The cluster contains 5 switches
---------------
Welcome to NOS CLI
user connected from ::FFFF:10.103.8.61 using ssh on abc.com
switch#
```

See Also **show running-config banner**

bind

Used to create a persistent binding between the logical FCoE port and the tengigabit or LAG port.

Synopsis **bind** {**tengigabitethernet** *rbridge-id/slot/port* | **mac-address** *address*}

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
mac-address *address*	Specifies a MAC address. The valid format is HH:HH:HH:HH:HH:HH.

Defaults None

Command Modes Interface configuration mode

Description When the FCoE logical port is automatically bound to a TE/LAG port, it is referred as dynamic binding. This binding is valid only till the FLOGI session is valid. The binding is automatically removed when CNA logs out.

If you want to create a persistent binding between the logical FCoE port and the tengigabit or LAG port, use the bind command. This will be stored in the configuration and retained across reboots.

Usage Guidelines Only one type of binding can be used for each physical port, so the tengigabit or LAG binding configuration will overwrite each other.

Examples

```
switch(config)# interface fcoe 1/1/55
switch(config-Fcoe-1/1/55)# bind tengigabitethernet 1/0/1
switch(config)# interface fcoe 1/1/56
switch(config-Fcoe-1/1/56)# bind mac-address 00:05:1e:c5:96:a4
```

See Also max-enodes

bpdu-drop enable

Drops STP/RSTP/MSTP and PVST/RPVST bridge protocol data units (BPDUs).

Synopsis **bpdu-drop enable**

no bpdu-drop enable

Operands None.

Defaults BPDU-drop is disabled by default.

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to prevent reception of any STP or PVST BPDUs on a interface. If such a BPDU is received on a interface that is bpdu-drop enabled, the interface is shut down.

Usage Guidelines Use the **no bpdu-drop enable** command to disable bpdu-drop.

Examples To enable bpdu dropping on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet178/0/9
switch(conf-if-te-178/0/9)# bpdu-drop enable
```

To disable bpdu dropping on a specific port-channel interface

```
switch(config)# interface port-channel 62
switch(conf-Port-channel-62)# no bpdu-drop enable
```

See Also **interface**

bridge-priority

Specifies the priority of the bridge.

Synopsis **bridge-priority** *priority* [*vlan vlan_id]*

no bridge-priority

Operands

priority	Specifies the bridge priority. The range of valid values is from 0 through 61440.
vlan vlan_id	Specifies the VLAN ID. Refer to "Description" below.

Defaults The default priority is 32768.

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.

If the VLAN parameter is not provided, the priority value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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.

This command does not function in VCS mode.

Examples To specify the bridge priority:

```
switch# 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**

cee

Applies a Converged Enhanced Ethernet (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 subconfiguration mode (gi, Port-channel, te).

Description Use this command to apply an existing CEE map on a specific interface.

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

Use the **no cee** command to remove the CEE Provisioning map.

Examples To apply a CEE map to a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# cee default
```

See Also **interface**, **cee-map (configuration)**, **channel-group**, **dot1x authentication**, **dot1x port-control**, **dot1x quiet-period**, **dot1x reauthentication**, **dot1x reauthMax**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**, **edge-loop-detection VLAN**, **edge-loop-detection port-priority**

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    6    7
     ---------------------------------------------
     PGID:    2    2    2    1    2    2    2    2
   FCoE CoS: None
   Enabled on the following interfaces
```

Usage Guidelines None

Examples None

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

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**

certutil import ldapca

Imports an LDAP CA certificate.

Synopsis **certutil import ldapca directory** *path* **file** *filename* **protocol** {*FTP* | *SCP*} **host** *remote_ip* **user** *user_acct* **password** *password*

no certutil ldapca

Operands

directory *path*	Specifies the path to the certificate.
file *filename*	Specifies the filename for the certificate.
protocol *FTP* | *SCP*	Specifies the protocol used to access the remote server.
host *remote_ip*	Specifies the IP address of the remote host.
user *user_acct*	Specifies the user name to access the remote host.
password *password*	Specifies the password to access the remote host.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to import a Lightweight Directory Access Protocol (LDAP) Certification Authority (CA) certificate from a remote server. This command supports FTP and SCP.

Usage Guidelines The **no certutil ldapca** deletes the LDAP CA certificates of all Active Directory servers.

Examples To import a certificate for LDAP:

```
switch# certutil import ldapca directory /usr/ldapcacert file cacert.pem protocol
SCP host 10.23.24.56 user admin password *****
```

To delete all LDAP CA certificates:

```
switch# no certutil ldapca
```

See Also **ldap-server host, ldap-server maprole, show cert-util ldapca, show running-config ldap-server, username**

certutil import syslogca

Imports a syslog server CA certificate.

Synopsis **certutil import syslogca protocol {FTP | SCP} host** *remote_ip* **user** *user_acct* **password** *password* **directory** *path* **file** *filename*

no certutil syslogca

Operands

protocol *FTP | SCP*	Specifies the protocol used to access the remote server.
host *remote_ip*	Specifies the IP address of the remote host.
user *user_acct*	Specifies the user name to access the remote host.
password *password*	Specifies the password to access the remote host.
directory *path*	Specifies the path to the certificate.
file *filename*	Specifies the filename (in .pem format) for the certificate.

Defaults None.

Command Modes Privileged EXEC mode.

Description Use this command to import a syslog CA certificate from a remote server. The certificate is required for secure syslog to function properly. Only one syslog CA certificate can be installed on a switch.

Usage Guidelines Use the **no certutil syslogca** to uninstall the syslog server CA Certificate.

Examples To import a syslog CA certificate:

```
switch# certutil import syslogca protocol SCP host 10.70.4.101 user testuser
password password directory /users/home40/testuser file cacert.pem
```

To delete the syslog CA certificate:

```
switch# no certutil syslogca
```

See Also None.

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. In Standalone mode, the range of valid values is from 1 through 64. In Brocade VCS Fabric mode, the range of valid values is from 1 through 6144.
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 subconfiguration mode (fo, gi, te).

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.

Usage Guidelines Only a maximum of 24 LAGs can be created. Be aware of 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.

Use the **no channel-group** command to remove the port-channel members.

Examples To set the channel-group number to 4 and the mode to *active* on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# channel-group 4 mode active
```

To set the channel-group number to 10, the mode to *passive*, and the type to brocade on a specific gigabitethernet interface:

```
switch(config)# interface gigabitethernet 170/0/1
```

```
switch(conf-if-gi-170/0/1)# channel-group 10 mode passive brocade
```

See Also interface

chassis beacon

Controls the flashing LED beacon on the switch.

Synopsis **chassis beacon** {**enable** | **disable**}

Operands

enable	Enables the chassis beacon LED.
disable	Disables the chassis beacon LED.

Defaults None

Command Modes Privileged EXEC mode

Description Use the **chassis beacon** command to toggle the flashing LED locator on the Brocade switch. This makes finding the switch easier in large data centers.

Usage Guidelines None

Examples To enable the chassis beacon:

```
switch# chassis beacon enable
Chassis Beacon has been enabled
```

To disable the chassis beacon:

```
switch# chassis beacon disable
Chassis Beacon has been disabled
```

See Also None

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**

chassis fan airflow-direction

Specifies the direction of airflow through the chassis based on physical PSU and fans.

Synopsis **chassis fan airflow-direction** [**port-side-intake** | **port-side-exhaust**]

Operands

port-side-intake	Specifies the airflow to enter the switch.
port-side-exhaust	Specifies the airflow to exit the switch.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to configure the fan airflow direction to match the physical PSU and fans installed in the system.

Usage Guidelines This command must only be used after you purchase and install the appropriate fan/power supply that provides the desired airflow direction in the switch. Please contact your Brocade Sales Representative to obtain the correct part numbers and pricing.

When the **chassis fan airflow-direction** command is issued, the switch will not recognize the configuration change until the switch is rebooted.

Only one (1) configuration change is accepted per reboot. This means that even if this command is entered multiple times, only the first configuration change entered will be effective after rebooting.

The switch serial number is registered with Brocade and the information recorded in the Brocade database about that switch includes the airflow orientation at the time of shipment.
Any subsequent change in airflow direction is not recorded in the Brocade database. This means that if you request a Return Merchandise Authentication (RMA) for the switch, the replacement switch will be sent with the original orientation.

Examples To specify the fan airflow-direction:

```
switch# chassis fan airflow-direction port-side-exhaust
Previous configuration : port-side-intake
Current configuration  : port-side-exhaust
System fan airflow-direction changes will be effective after reboot!!
```

See Also None

cidrecov

Recovers data from Chassis ID cards if possible.

Synopsis cidrecov

Operands There are no operands for this command.

Command Modes Privileged EXEC mode.

Description Run this command if you receive an error or warning raslog that instructs you to run the command.

Two chassis ID (CID) cards contain data necessary for system operation. Each CID contains two Serial Electronically Erasable Programmable Read Only Memory (SEEPROM) devices. If data on either card becomes corrupt or mismatched, a regularly run CID audit writes messages to *raslog*. Follow the instructions in the messages. Mismatched data can be reset, and corrupt data can sometimes be recovered if the corrupt data is on the non-critical SEEPROM.

Usage Guidelines This command is supported only on the Brocade VDX 8770-4 and Brocade VDX 8770-8 platforms.

Examples Example 1: Non-critical SEEPROM is inaccessible or corrupt, but recovery becomes possible:

```
sw0# cidrecov

CID 1 Non-Critical Seeprom  is Inaccessible or Corrupted.

    CID Non-Critical Seeprom Problem Details

CID 1 Non-Critical Seeprom IP address Control Data Checksum Bad !!!!


CID 1 IP address Control Data:
Version: 0xa
Checksum: 0x0
Size: 0x3

CID 2 IP address Control Data:
Version: 0xa
Checksum: 0x7
Size: 0x3

***WARNING: Recovering IP Data May Affect Both IP  Control and IP Records ***
Backup Current Data Displayed Below If Needed.

CID 1 Chassis Name: VDX8770-4
CID 2 Chassis Name: VDX8770-4
CID 1 IP address Control Data:
Version: 0xa
Checksum: 0x0
Size: 0x3

CID 2 IP address Control Data:
Version: 0xa
Checksum: 0x7
Size: 0x3
```

```
IP address Record 1  on CID 1
1st IP Address: 10.17.19.53
1st IP Mask: 255.255.240.0
2nd IP Address: 10.17.19.54
2nd IP Mask: 255.255.240.0
Gateway Address: 10.17.16.1

IP address Record 1  on CID 2
1st IP Address: 10.17.19.53
1st IP Mask: 255.255.240.0
2nd IP Address: 10.17.19.54
2nd IP Mask: 255.255.240.0
Gateway Address: 10.17.16.1

IP address Record 2  on CID 1
1st IP Address: 10.17.19.52
1st IP Mask: 255.255.240.0
2nd IP Address: 0.0.0.0
2nd IP Mask: 0.0.0.0
Gateway Address: 0.0.0.0

IP address Record 2  on CID 2
1st IP Address: 10.17.19.52
1st IP Mask: 255.255.240.0
2nd IP Address: 0.0.0.0
2nd IP Mask: 0.0.0.0
Gateway Address: 0.0.0.0


        CID Recovery Options

0. Exit

1. Recover with default values

2. Recover BAD from GOOD

Enter Selection > 2
Copy IP Data table...
    Copy 384 bytes from CID 2 to CID 1, num blks 1 resid 128
    Read block 1 from CID 2 succeeded
    Write block 1 to CID 1 succeeded
    Read last block from CID 2 succeeded
    Write last block to CID 1 succeeded
    copy successful

Copy succeeded for all data types attempted
IP Address CID Recovery completed.
```

Example 2: Non-critical SEEPROM is inaccessible or corrupt, but recovery is not possible:

```
sw0# cidrecov

CID 1 Non-Critical Seeprom  is Inaccessible or Corrupted.

    CID Non-Critical Seeprom Problem Details

CID 1 Non-Critical Seeprom  Read Failed.
Recovery is not possible. Please contact Brocade Technical Support for
replacement of the inaccessible CID(s).
```

Example 3: Critical SEEPROM data is mismatched, recovery is not possible:

```
sw0# cidrecov

CID 1 and CID 2 Critical Seeprom Data is Mismatched.

    CID Seeprom Problem Details

CID Seeprom Chassis Serial Number Mismatch.
CID 1 Serial Number: BYP3G15G00N
CID 2 Serial Number: BYP3G17H00P

Recovery is not possible. Please contact Brocade Technical Support for
replacement of the corrupted CID(s).
```

cipherset

Configures FIPS-compliant ciphers for LDAP and SSH protocols.

Synopsis **cipherset {ldap | ssh}**

Operands

ldap	Specifies secure LDAP ciphers.
ssh	Specifies secure SSH ciphers.

Defaults By default, there are no restrictions exist on LDAP and SSH ciphers.

Command Modes Privileged EXEC mode

Description Use this command to configure secure ciphers that are FIPS compliant for the Lightweight Directory Access Protocol (LDAP) and Secure Shell (SSH). A switch must be configured with secure ciphers for SSH before that switch can be FIPS compliant. If LDAP authentication is to be used, the LDAP ciphers are also required before a switch can be FIPS compliant.

The secure LDAP ciphers are AES256-SHA, EAS128-SHA, and DES-CBC3-SHA. The secure SSH ciphers are HMAC-SHA1 (mac), 3DES-CBC, AES128-CBC, AES192-CBC, abd AES256-CBC.

Usage Guidelines This command applies only in the standalone mode. This command can be entered only from a user account with the admin role assigned.

Examples To configure secure LDAP ciphers and secure SSH ciphers:

```
switch# cipherset ldap
ldap cipher list configured successfully
switch# cipherset ssh
ssh cipher list configured successfully
```

See Also **fips root disable, fips selftests, fips zeroize, prom-access disable, show prom-access**

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.

This command does not function in VCS mode.

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:

```
switch# configure terminal
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# cisco-interoperability disable
```

See Also None

class

Configure a class-map in a policy-map by providing the class-map name and policing parameters. The class-map must have been created and associated with match criteria using the **class-map** command (refer to "qos cos" on page 329.

Synopsis **class** *class-map name*

no class *class-map name*

[**no**] **police cir** *cir-rate*| **cbs** *cbs-size* | **eir** *eir-rate* | **ebs** *ebs-size* | **set-priority** *priority-map-name* | **conform-set-dscp** *dscp-num* | **conform-set-prec** *prec-num* | **conform-set-tc** *trafficclass* | **exceed-set-dscp** dscp-num | **exceed-set-prec** *prec-num* | **exceed-set-tc** *trafficclass* |

Operands The following are policing parameters for configuring the class-map.

police cir *cir-rate*	Committed information rate. Acceptable values are in multiples of 40000 in the range 40000 - 40000000000 bps. This is a mandatory parameter for configuring a class-map.
no police cir	Removes police CIR.
cbs *cbs-size*	Controlled burst size. Acceptable values are 1250 - 5000000000 bytes in increments of 1 byte. This is a mandatory parameter for configuring a class-map.
eir *eir-rate*	Excess information rate. Acceptable values are in multiples of 40000 in the range 0 - 40000000000 bps.
ebs *ebs-size*	Excess burst size. Acceptable values are 1250 - 5000000000 bytes in increments of 1 byte.
set-priority *name*	The priority-map name that you are including in the policy-map. Refer to "police-priority-map" on page 310.
conform-set-dscp	Specifies that traffic with bandwidth requirements within the rate configured for CIR will have packet DSCP priority set to the value specified by the *dscp-num* variable. Acceptable values for *dscp-num* are 0-63.
conform-set-prec	Specifies that traffic with bandwidth requirements within the rate configured for CIR will have packet IP precedence value (first 3 bits of DSCP) set to the value in the *prec-num* variable. Acceptable values for *prec-num* are 0-7.
conform-set-tc	Specifies that traffic with bandwidth requirements within the rate configured for CIR will have traffic class (internal queue assignment) set to the value in the *trafficclass* variable. Acceptable values for *trafficclass* are 0-7.
exceed- set-dscp	Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and sent to the EIR bucket will have packet IP precedence set to the value in the *prec-num* variable. Acceptable values for *prec-num* are 0-7.
exceed-set-prec	Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and sent to the EIR bucket will have packet IP precedence set to the value in the *prec-num* variable. Acceptable values for *prec-num* are 0-7.

exceed-set-tc Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and is in the limit of what is configured for EIR will have its traffic class (internal queue assignment) set to the value in the *trafficclass* variable. Acceptable values for *trafficclass* are 0-7.

Defaults No created policy-map.

Command Modes global configuration mode

policy-map configuration (config-policymap) mode

configure policy-map classification (config-policymap-class) mode

configure policy-map classification police (config-policymap-class-police) mode

Description Use this command to configure a class-map for a police policy-map. When you launch the **class** command while in config-policymap mode (refer to "policy-map" on page 311) for a policy, the system is placed in configure policy-map classification (config-policymap-class) mode. At this point, you can configure QoS and policing parameters for the class-map.

Usage Guidelines This command configures a class-map for a police policy-map with QoS and policing parameters for inbound or outbound traffic. These parameters define cir, cbr, ebr, and eir rates and actions to occur when traffic conforms or exceeds set rates. For more details on these parameters, refer to the "Port-based Policer" section in the QoS Configuration chapter of the *Network OS Administrator's Guide*. Each policy-map can contain one class-map. Use the **no policy-map** *name* command while in global configuration mode to remove the policy-map. Associate the policy-map to the interface for inbound or outbound direction with the **service-policy** command (refer to "service-policy" on page 393).

When you are in config-policymap-class mode launching the **police cir** *cir-rate* command places the system in config-policymap-class-policemode for the configured class-map. At this point, you can add or remove additional policing parameters for the class-map. Use the **no police** command while in config-policymap-class mode to remove all policing parameters for the class-map. Use the **no police** command followed by a policing parameter name to remove a specific parameter.

NOTE
The cir and cbs parameters are the mandatory for configuring a class-map. Other parameters are optional. If optional parameters are not set then they will be treated as disabled. To delete the mandatory cir or cbs parameters, you must delete all Policer parameters while in the policy-map class configuration mode using the **no police** command.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To configure a class-map called "default" within a policy-map when in config-policymap-class mode and configure policing parameters for the class-map you can group all parameters after the **police cir** command:

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police  cir 40000 cbs  5000 eir
40000  ebs  3000  set-priority  pmap1  conform-set-dscp   61   conform-set-tc
7 exceed- set-dscp  63  exceed- set-tc   3
switch(config-policymap-class-police)#
```

As an alternate method to configure policing parameters for a class-map, enter the **police cir** *cir-rate* command to place the system in config-policymap-class-police mode, then enter individual parameters:

```
switch (config-policymap-class)# police  cir 40000
switch(config-policymap-class-police)# cbs 50000
switch(config-policymap-class-police)# eir 800000
switch(config-policymap-class-police)# ebs 400000
switch(config-policymap-class-police)# conform-set-tc 3
switch(config-policymap-class-police)# exceed-set-prec 4
```

To delete the mandatory cir or cbs parameter, you must delete all Policer parameters while in the policy-map class configuration mode using the following example:

```
switch(config-policymap-class)# no police
```

To delete any parameter, use the **no** operand while in the config-policymap-class-police configuration mode. The following example removes the EBS setting.

```
switch(config-policymap-class-police)# no ebs
```

To remove the class-map "default" from the policy-map while in config-policymap mode:

```
switch(config-policymap)# no class default
```

See Also police-priority-map, policy-map, qos cos, service-policy

class-map

Creates a classification map or “class-map” to classify traffic based on configured match criteria.

Synopsis **class-map** *class-map name*

no class-map *class-map name*

match criteria

Operands

class-map *name*	Name of classification map
match criteria	match any

Defaults There is no explicit class-map applied.

Command Modes global configuration mode

class-map configuration mode (config-classmap)

Description Use this command to classify traffic based on match criteria. When you launch the **class-map** command, the system is placed in config-classmap mode for the configured map. At this point, you can provide match criteria for the class. The only available match criteria at this time is “match any.”

Usage Guidelines This command creates a classification map. Use the *match criteria* operand while in config-classmap mode to configure the match criteria for the class. Use the **no map class-map** *name* command while in global configuration mode to remove the classification map.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To create a classification map and place system into config-classmap mode:

```
switch(config)# class-map default
switch(config-classmap)#
```

To configure “match any” match criteria for the class while in config-classmap mode:

```
switch(config-classmap)# match any
```

NOTE
The class map created using *switch(config)#* **class map** becomes the default class-map and cannot be removed using the **no class-map** command. You can remove a class-map from a policy map however.

See Also **show running-config class-map**

clear arp-cache

Clears the ARP statistics cache on the host.

Synopsis **clear arp-cache** [**interface gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* [*no-refresh*]] | [**ip** *ip-address* [*no-refresh*] | [*no-refresh*]]

Operands

interface	Clears the ARP cache for the specified interface only.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port 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-refresh	Do not refresh the ARP.
no-refresh	Do not refresh the ARP.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples None

See Also None

clear counters (IP)

Clears the IP counter statistics on all interfaces on the switch.

Synopsis **clear counters** {**all** | **access-list ip** *access_list_name* | **interface** {**port-channel** *number* | **fibrechannel** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **fortygigabitethernet** *rbridge-id/slot/port*} | **slot-id** *number* | **vlan** *vlanId* | **ve** *vlanId*} {**in** | **out**}

Operands

all Specifies to clear statistics on all interfaces.

access-list ip *access_list_name* Specifies the name of the IP access list.

interface Specifies the use of the *port-channel*, *fibrechannel*, *gigabitethernet* or *tengigabitethernet* keyword.

port-channel *number*
Specifies the port-channel number. The range of valid values is from 1 through 64 in standalone mode and from 1 through 6144 in VCS mode.

fibrechannel Specifies a valid Fibre Channel interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet Specifies a valid 1 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet Specifies a valid 10 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

fortygigabitethernet Specifies a valid 40 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

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

vlan *vlanId* Specifies the VLAN interface to which the ACL is bound.

ve *vlanId* Specifies the Virtual Ethernet interface to which the ACL is bound.

in | **out** Specifies the binding direction (ingress or egress).

Defaults None

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 Brocade VDX switches, the slot number is always 0 (zero).

Examples To clear the statistics for 10 Gbps Ethernet interface 5/0/1:

```
switch# clear counters interface tengigabitethernet 5/0/1
```

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 (MAC)

Clears the MAC counter statistics on all interfaces on the switch.

Synopsis **clear counters** {**all** | **access-list mac** *access_list_name* | **interface** {**port-channel** *number* | *fibrechannel rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **fortygigabitethernet** *rbridge-id/slot/port*} | **slot-id** *number* | **vlan** *vlanId* | **ve** *vlanId*} {**in | out}**

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*, *fibrechannel*, *gigabitethernet* or *tengigabitethernet* keyword.
port-channel *number*	Specifies the port-channel number. The range of valid values is from 1 through 64 in standalone mode and from 1 through 6144 in VCS mode.
fibrechannel	Specifies a valid Fibre Channel interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
fortygigabitethernet	Specifies a valid 40 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
vlan *vlanId*	Specifies the VLAN interface to which the ACL is bound.
ve *vlanId*	Specifies the Virtual Ethernet interface to which the ACL is bound.
slot-id *number*	Specifies the slot number of the linecard.
**in	out**	Specifies the binding direction (ingress or egress).

Defaults None

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 Brocade VDX switches, the slot number is always 0 (zero).

Examples To clear the statistics for 10 Gbps Ethernet interface 5/0/1:

```
switch# clear counters interface tengigabitethernet 5/0/1
```

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* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*]]

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 64 in standalone mode and from 1 through 6144 in VCS mode.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

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 tengigabitethernet 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**

clear counters storm-control

Clears counters about traffic controlled by configured rate limits.

synopsis **clear counters storm-control**

clear counters storm-control broadcast [**interface** {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *bridge-id/slot/port*]

clear counters storm-control interface {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*

clear counters storm-control multicast [**interface** {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*]

clear counters storm-control unknown-unicast [**interface** {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*]

operands **clear counters storm-control**
Clears all BUM-related counters in the system.

clear counters storm-control broadcast
Clears all BUM-related counters in the system for the broadcast traffic type.

clear counters storm-control interface *type rbridge-id/slot/port*
Clears all BUM-related counters in the system for the specified interface. You must specify an interface type, followed by the rbridge-id/slot/port.

show storm-control multicast
Clears all BUM-related counters in the system for the multicast traffic type.

clear counters storm-control unknown-unicast
Clears all BUM-related counters in the system for the unknown-unicast traffic type.

interface *type rbridge-id/slot/port*
Specifies an interface type, followed by the rbridge-id/slot/port, for which to clear all BUM-related counters in the system for the specified traffic type. Use this option to clear counters on a per-port basis.

Default None.

Command Modes Privileged EXEC mode.

Description Clears the counters for broadcast, unicast, and unknown-multicast (BUM) traffic for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interfaces.

Usage Guidelines None.

Examples To clear counters for broadcast traffic on the tengigabitethernet interface 102/4/1:

```
switch# clear counters storm-control broadcast interface tengigabitethernet
102/4/1
```

To clear counters for all traffic types enabled on the tengigabitethernet interface 102/4/1:

```
switch# clear counters storm-control interface tengigabitethernet 102/4/1
```

To clear counters for all multicast traffic in the system:

```
switch# clear counters storm-control multicast
```

To clears all BUM-related counters in the system:

```
switch# clear counters storm-control
```

clear dot1x statistics

Clears all dot1x statistics.

Synopsis **clear dot1x statistics**

Operands None

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

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 [gigabitethernet** *rbridge-id/slot/port* **| tengigabitethernet** *rbridge-id/slot/port*]

Operands

gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples To clear dot1x statistics on a port:

```
switch# clear dot1x statistics interface tengigabitethernet 0/16
```

See Also **clear dot1x statistics**

clear edge-loop-detection

Re-enables all ports disabled by ELD and clears all ELD statistics.

Synopsis **clear edge-loop-detection**

Operands None

Defaults None

Command Modes ELD configuration mode.

Description Use this command to re-enable all ports shut down by ELD on the Brocade VCS Fabric cluster and to clear all ELD statistics. This operation is typically performed after correcting a configuration error that caused ELD to disable ports.

Usage Guidelines This command applies to Brocade VCS Fabric mode only.

This functionality detects Layer 2 loops only.

Example None

See Also **protocol edge-loop-detection, show edge-loop-detection interface, show edge-loop-detection rbridge-id**

clear fcoe login

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

Synopsis **clear fcoe login** [**interface fcoe** *rbridge-id/slot/port*] | [**vlan** *vlan_id*] | [**interface tengigabitethernet** *rbridge-id/slot/port]* | [**vfid** *vfid*] | [**device** *device-wwn*]

Operands

interface fcoe	The VN number/VCS node mapped ID/logical port number for the virtual-fabric.
rbridge-id	Specifies the ID of the routing bridge. 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. Refer to "Usage Guidelines" below.
interface tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
vfid *vfid*	The virtual fabric ID for the device.
device *device-wwn*	The World Wide Name of the device.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples

```
switch#clear fcoe login interface fcoe 1/1/1
switch#clear fcoe login device 10:00:00:05:1e:8e:be:40
switch#clear fcoe login interface tengigabitethernet 1/0/1
switch#clear fcoe login vlan 1002
switch#clear fcoe login vfid 1
```

See Also None

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 port-channel** *number* | **interface vlan** *vlan_id*} | **interface tengigabitethernet** *rbridge-id/slot/port* | **interface gigabitethernet** *rbridge-id/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 tengigabitethernet
Specifies a valid external 10 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

interface gigabitethernet
Specifies a valid 1 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

interface 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 Brocade VCS Fabric mode.

interface vlan *vlan_id* Specifies which VLAN interface to display the snooping configuration related information. Refer to "Usage Guidelines" below.

Defaults None

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 On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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

```
switch# clear ip igmp groups
```

See Also None

clear ip igmp statistics

Clears statistical information related to the IGMP protocol module.

Synopsis **clear ip igmp statistics interface vlan** *vlan_id*

Operands **interface vlan** *vlan_id* Specifies which VLAN interface to clear the statistical information. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the statistics information in the IGMP database.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To clear statistics information for a VLAN in the IGMP protocol:

```
switch# clear ip igmp statistics interface vlan 11
```

See Also None

clear ip ospf

Clears OSPF process, counters, neighbors, or routes.

Synopsis **clear ip ospf all**

clear ip ospf counters {all | FortyGigabitEthernet *rbridge-id/slot/port* **| GigabitEthernet** *rbridge-id/slot/port* **| Port-channel** *number* **| TenGigabitEthernet** *rbridge-id/slot/port* **| ve** *vlan#***}**

clear ip ospf neighbor {*A.B.C.D* | **all**}

clear ip ospf routes {*A.B.C.D* | **all**}

Operands

clear ip ospf all Restarts the OSPF process.

counters Clears all counters or clears the counters of an interface that you specify:

- **all** Clears all counters.
- **FortyGigabitEthernet** *rbridge-id/slot/port* Clears counters on the specified, valid 40-Gbps port interface.
  - *rbridge-id* Specifies the ID of the routing bridge. This operand is not valid in standalone mode.
  - *slot* Specifies a valid slot number.
  - *port* Specifies a valid port number.
- **GigabitEthernet** *rbridge-id/slot/port* Clears counters on the specified, valid 1-Gbps Ethernet interface
  - *rbridge-id* Specifies the ID of the routing bridge.
  - *slot* Specifies a valid slot number.
  - *port* Specifies a valid port number.
- **Port-channel** *number* Clears counters on the specified, valid port-channel number. The range of valid values is 1 through 6144.
- **tenGigabitEthernet** *rbridge-id/slot/port* Clears counters on the specified, valid 10-Gbps Ethernet interface.
  - *rbridge-id* Specifies the ID of the routing bridge.
  - *slot* Specifies a valid slot number.
  - *port* Specifies a valid port number.
- **ve** *vlan#* Clears counters on the specified vlan number.

neighbor Clears the specified neighbor, or clears all neighbors.

- *A.B.C.D* Specifies the IP address of the neighbor to clear.
- **all** Clears all neighbors.

routes Clears matching routes or clears all routes.

- *A.B.C.D* Clears all routes that match the prefix and mask that you specify.
- **all** Clears all routes.

Default None.

Command Modes Privileged EXEC mode.

Examples To restart the OSPF processes:

```
switch# clear ip ospf all
```

clear ip route

Clears IP routes.

Synopsis **clear ip route** {*A.B.C.D/M* | **all** | **slot** *line_card_number*}

Operands

A.B.C.D/M	Clears the route specified by this IPv4 address/length.
all	Clears all routes from the routing table in IP route management.
slot *line_card_number*	Clears the route specified by this line card number.

Default None.

Command Modes Privileged EXEC mode.

Description Clears either all IP routes in IP routing tables or clears a route that you specify.

Usage Guidelines None.

Examples To clear the IP route specified by the prefix 192.158.1.1/24:

```
sw0# clear ip route 192.158.1.1/24
```

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 64 in standalone mode and from 1 through 6144 in VCS mode.
counters	Clears traffic counters.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

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

```
switch# clear lacp 10 counters
```

See Also show lacp counters

clear lacp counters

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

Synopsis **clear lacp counters**

Operands None

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples To clear the counters for all port-channels:

```
switch# clear lacp counters
```

See Also **show lacp counters**

clear lldp neighbors

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

Synopsis **clear lldp neighbors interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

interface		Use this keyword to specify the interface using this operand followed by the slot or port number.
	tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.

Defaults None

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 lldp neighbors**

clear lldp statistics

Clears LLDP statistics for all interfaces or a specified interface.

Synopsis **clear lldp statistics interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

interface		Use this keyword to specify the interface using this operand followed by the slot or port number.
	tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines If the **interface** operand is not specified, this command clears all the LLDP statistics on all interfaces.

Examples To clear all the LLDP statistics for all interfaces:

```
switch# clear lldp statistics
```

See Also **show lldp statistics**

clear logging auditlog

Clears the audit log system messages.

Synopsis **clear logging auditlog** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode.
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 audit log messages.

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

Examples To clear the audit log messages on the local switch:

```
switch# clear logging auditlog
```

See Also clear logging raslog, logging auditlog class, show logging auditlog

clear logging raslog

Clears RASlog messages from the switch.

Synopsis **clear logging raslog [message-type {DCE | SYSTEM}]** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

message-type	**Clears RASlog messages of the specified type.**	
	SYSTEM	Clears system messages.
	DCE	Clears DCE application messages.
	rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include:
		rbridge-id — Specifies the ID of the routing bridge. This option is not valid in standalone mode.
		all — Specifies all switches in the fabric.

Defaults Clear all RASlog messages of on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to clear the saved RASlog messages.

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

This command is not supported on the standby management module.

Examples To clear all RASlog messages on the local switch:

```
switch# clear logging raslog
DCE Raslogs are cleared
SYSTEM Raslogs are cleared
```

To clear all DCE messages on the local switch:

```
switch# clear logging raslog message-type DCE
DCE Raslogs are cleared
```

To clear all SYSREM messages on the local switch:

```
switch# clear logging raslog message-type SYSTEM
SYSTEM Raslogs are cleared
```

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

clear sflow statistics

Clears all sFlow statistics.

Synopsis **clear sflow statistics**

Operands None

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples To clear sFlow statistics:

```
switch# clear sflow statistics
```

See Also None

clear spanning-tree counter

Clears all spanning-tree counters on the interface.

Synopsis **clear spanning-tree counter** [**interface** | **port-channel** *number* | **tengigabitethernet** *slot/port* | *gigabitethernet 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 64.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines If the **interface** operand is not specified, spanning-tree counters are cleared for all interfaces.

This command does not function in VCS mode.

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**

clear support

Removes support data on the switch.

Synopsis **clear support** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified RBridges. This option is not valid in standalone mode and currently not supported.
rbridge-id	Specifies the ID of the routing bridge.
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 This command is supported only on the local switch.

Examples To remove core files from the local switch:

```
switch# clear support
```

See Also autoupload, copy support, show support

clear vrrp statistics

Clears VRRP statistics.

Synopsis **clear vrrp statistics**

clear vrrp statistics [interface {FortyGigabitEthernet *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **TenGigabitEthernet** *rbridge-id/slot/port***}]**

clear vrrp statistics [session *VRID* **all]**

Operands **interface** Clears statistics for an interface that you specify.

FortyGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 40-Gbps port interface.

rbridge-id Specifies the ID of the routing bridge.
This operand is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

GigabitEthernet *rbridge-id/slot/port*
Specifies a valid 1-Gbps Ethernet interface

rbridge-id **Specifies the ID of the routing bridge.**

slot Specifies a valid slot number.

port Specifies a valid port number.

TenGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 10-Gbps Ethernet interface.

rbridge-id **Specifies the ID of the routing bridge.**

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan* Specifies the vlan number.

session *VRID* Specifies the virtual group ID on which to clear statistics. Range is 1 to 128.

Default None.

Command Modes Privileged EXEC mode.

Description Clears VRRP session statistics for all virtual groups, for a specified interface or for a specified virtual group. To clear all statistics, use the **clear vrrp statistics** command with no operands.

Usage Guidelines This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** interface type.

Examples To clear all VRRP statistics for all virtual groups:

```
switch# clear vrrp statistics
```

To clear statistics for a TenGigabitEthernet interface that has an rbridge-id/slot/port of 121/0/50:

```
switch# clear vrrp stastistics interface tengigabitethernet 121/0/50
```

To clear statistics for a session for a VRRP virtual group called “vrrp-group-25”

```
switch# clear vrrp session 25
```

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. Valid date and time settings range from January 1, 1970 to January 19, 2038.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to set the local clock.

Usage Guidelines An active NTP server, if configured, automatically updates and overrides the local clock time. Network Time Protocol (NTP) commands must be configured on each individual switch.

Examples To set the date and time to March 17, 2010, 15 minutes past noon:

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

See Also **clock timezone, ntp server, show clock**

clock timezone

Sets the time zone based on region and longitudinal city.

Synopsis **clock timezone** *region/city*

no clock timezone

Operands

region	Specifies the region's time zone.
city	Specifies the city's time zone.

Defaults None

Command Modes Privileged EXEC mode

Description Sets the local clock time zone.

Usage Guidelines Regions include the following countries: Africa, America, Pacific, Europe, Antarctica, Asia, Australia, Atlantic, Indian, and longitudinal city. For a complete listing of supported regions and cities, refer to Appendix C in the *Network OS Administrator's Guide*.

By default, all switches are in the Greenwich Mean Time (GMT) time zone. The **no** operand removes the timezone setting for the local clock.

Network Time Protocol (NTP) commands must be configured on each individual switch.

The region name and city name must be separated by a slash (/).

After upgrading your switch to a new Network OS version, you may need to reset the time zone information.

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

```
switch# clock timezone America/Los_Angeles
```

See Also **clock set, ntp server, show clock**

copy

Copies configuration data.

Synopsis **copy** *source_file destination_file*

Operands

source_file **The source file to be copied. Specify one of the following options:**

- **default-config** **The default configuration.**
- **running-config** **The running configuration.**
- **startup-config** **The 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.

destination_file The destination file. Specify one of the following options:

- **default-config** The default configuration.
- **running-config** The running configuration.
- **startup-config** The 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.

IPv4 and IPv6 addresses are supported.

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]: 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 default-config startup-config, copy running-config startup-config, delete, dir, rename, show file, show running-config, show startup-config

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.

The command behaves differently depending on whether the switch is in standalone mode or part of a Brocade VCS fabric.

In standalone mode, all interfaces are shut down. When the switch comes back up, the restored default configuration is used. The following parameters are unaffected by this command:

- Interface management IP address
- Software feature licenses installed on the switch

In VCS Fabric mode, all interfaces remain online. The restored default configuration is applied with the exception of the following parameters:

- Interface management IP address
- Software feature licenses installed on the switch
- VCS mode configuration
- Virtual IP address

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, rename, show file, show running-config, show startup-config**

copy running-config startup-config

Copies the running configuration to the startup configuration.

Synopsis **copy running-config startup-config** [**display-command**]

Operands **display-command** Displays the configuration commands during the copy operation

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 This command is supported only on the local switch.

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 **copy, copy default-config startup-config, delete, dir, rename, show file, show running-config**

copy support

Copies support data to a remote host or a USB device.

Synopsis **copy support { usb | ftp | scp } user** *user_name* **password** *password* **host** *ip_address* **directory** *dir* **[timeout** *multiplier*] **[rbridge-id {***rbridge-id* | **all}]**

Operands

ftp | scp | usb	**Specifies the File Transfer Protocol (ftp), the Secure Copy Protocol (scp), or the USB directory.**
user *username*	**Specifies the user login name for the server.**
password *password*	**Specifies the account password.**
host *host_ip*	**Specifies the host IP address in IPv4 or IPv6 format.**
directory dir	*Specifies a fully qualified path* **to the directory where the support data will be stored.**
timeout *multiplier*	Specifies a timeout multiplier. Valid multipliers are 1 through 5. When a timeout multiplier is specified, the default timeout value for each module is multiplied by the specified timeout value.
rbridge-id	Executes the command on the specified switches. This option is not valid in standalone mode and currently not supported.
rbridge-id	Specifies the ID of the routing bridge.
all	Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to upload support data to an external host on to an attached USB device. The support data is saved in the following format:

switchname-IPaddress-slotnumber-cputype-timestamp.modulename.txt.ss.gz

Example: sw0-10.123.10.5-S5cp-201204081630.0S.txt.ss.gz

Usage Guidelines Pagination is not supported with this command. Use the more option to display the output one page at a time.

Examples To upload support data to a remote host:

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

To save support data on an attached USB device:

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

See Also **clear logging raslog, copy support-interactive, show support**

copy support-interactive

Copies support data interactively.

Synopsis **copy support-interactive**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command copies support data interactively. The command interface prompts you for the following information:

- Server Name or IP Address (IPv4 only)
- Protocol (FTP or SCP)
- User login name
- Password
- Directory
- Brocade VCS Fabric support
- Module timeout multiplier

Usage Guidelines This command is functionally equivalent to the **copy support** command.

Answering **Y** to the Brocade VCS Fabric support prompt indicates that your switch is in Brocade VCS Fabric mode. Support data will be copied from all nodes in the fabric.

Examples To upload support data interactively:

```
switch# copy 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
Module timeout multiplier[Range:1 to 5.Default:1]:2
copy support start
Saving support information for chassis:sw0, module:RAS...
(output truncated)
```

See Also **clear support, show copy-support status**

database-overflow-interval

Configures frequency for monitoring database overflow.

Synopsis **database-overflow-interval** *interval*

Operands

interval	Time interval (in seconds) at which the device checks to see if the overflow condition has been eliminated. The Range is 0 to 86400.

Default 0. If the router enters OverflowState, you must reboot before the router leaves this state.

Command Modes Router configuration mode.

Description Time (in seconds) after a router that has entered the OverflowState can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

For more information, refer to RFC 1765.

Usage Guidelines Use the **no** parameter to disable the overflow interval configuraion.

Examples To configure a database-overflow interval of 60 seconds:

```
switch(conf-ospf-router)# database-overflow-interval 60
```

See Also external-lsdb-limit

debug arp

Displays the ARP traffic.

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

Operands

interface	Displays the ARP traffic for the specified interface only.
interface-type	Network interface type (tengigabitethernet, gigabitethernet, port-channel, or VLAN interface).
interface-number	Layer 2 or Layer 3 interface number.
count *value*	Stops display after display count packets. The range of valid values is from 1 through 32256.
tx	Counts only transmitted packets.
rx	Counts only received packets.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples None

See Also None

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** *value* | **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, port-channel, or VLAN).
interface-number	Layer 2 or Layer 3 interface number.
count *value*	Stops display after display count packets. The range of valid values is from 1 through 32256.
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 None

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 None

Examples None

See Also None

debug ip igmp

Displays all IGMP information.

Synopsis **debug ip igmp** {**all** | **group** *A.B.C.D* | **interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/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.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
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 64 in standalone mode and from 1 through 6144 in VCS mode.
vlan *vlan_id*	Specifies which VLAN interface to display the snooping configuration related information. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples None

See Also None

debug ip ospf

Enables debugs.

Synopsis **debug ip ospf** {**adj** | **error** | **events** | **flood** | **log-debug-message** | **log-empty-lsa** | **ls-id** *A.B.C.D* | **lsa-generation** | **max-metric** | **neighbor** *A.B.C.D* | **packet** | **retransmission** | **route** *A.B.C.D* | **spf**}

no debug ip ospf {**adj** | **error** | **events** | **flood** | **log-debug-message** | **log-empty-lsa** | **ls-id** *A.B.C.D* | **lsa-generation** | **max-metric** | **neighbor** *A.B.C.D* | **packet** | **retransmission** | **route** *A.B.C.D* | **spf**}

Operands

Adj	Adjacency related debugs.
Error	Displays possible errors encountered during time.
Events	Events-related debugs.
Flood	Flooding-related debugs.
log-debug-message	Debugs message logging.
log-empty-lsa	Empties LSA logging.
ls-id *A.B.C.D*	Link state ID (LSID) debugging for the link-state ID that you specify.
lsa-generation	LSA generation-related debugging.
max-metric	Stub Router Advertisement.
neighbor *A.B.C.D*	Neighbor debugging for the neighbor that you specify.
Packet	Packet debugs.
retransmission	Retransmission events.
Route *A.B.C.D*	Route debugs for the router that you specify.
Spf	SPF trace.

Default All debugs are disabled by default.

Command Modes Privileged EXEC mode.

Description Enables or disables various debug options.

Usage Guidelines Use the **no** parameter to disable a debug.

Examples To enable adjacency-related debugs:

```
switch# debug ip ospf adj
```

debug ip rtm

Enables debugs.

Synopsis **debug ip rtm** {*A.B.C.D* | **all** | **counters** {**clear** | **show**} **errors** | **dump** | **nexthop** | **port**}

Operands

A.B.C.D	Debugs the route specified by this IP address.
all	Enables all debugs.
counters	Enables debug counters.
clear	Clears debug counters.
show	Shows debug counters.
dump	Shows database dump.
errors	Enables internal error debugs.
nexthop	Enables next-hop debugs.
port	Enables port database debugs.

Default None.

Command Modes Privileged EXEC mode.

Description Enables any or all debugs for IP route management.

Usage Guidelines None.

Examples To debug the route specified by the IP address 192.145.12.1:

```
sw0# debug ip rtm 192.145.12.1
```

To show a database dump:

```
sw0# debug ip rtm dump

Interface       IP-Address      OK?  Method Status     Protocol VRF
Gi 190/0/1      0xbe2a640c      YES  manual up         up       default-vrf
Ve 128          0xa52a800c      YES  manual admin/down up       default-vrf
Ve 1001         0x0a010101      YES  manual admin/down up       default-vrf
Ve 1001         0x65010101      YES  manual admin/down up       default-vrf
Lo 1            0xa02a0c0c      YES  manual up         up       default-vrf
mgmt 1          0x0a14eabe      YES  manual up         up       default-vrf
IP Static Routing Table - 1 entries:
addr: 0x1021f4b8, top 0x1021f590, count 1, default 0 ffffffff
        type 2
Route_pool:
pool: 101e3bd0, unit_size: 32, initial_number:128, upper_limit:2000000000
  total_number:128, allocated_number:1, alloc_failure 0
  flag: 0, pool_index:1, avail_data:102207b8
Route Entry Pool:
pool: 101e3c80, unit_size: 432, initial_number:128, upper_limit:2000000000
  total_number:128, allocated_number:1, alloc_failure 0
  flag: 0, pool_index:1, avail_data:10221950
Nexthop Settings
```

```
Update: no, Update-always no, Update-Timer 0 Check-Nexthops no
Recur: yes, Levels 3, Default-enable no
vrf-count 0, vrf-resolved yes
Protocols: < connected>
Nexthops List
 [7] 0xa14e801 hash 7 paths 1 upd last-update-time 0 -> 0xa14e801 mgmt 1
Nexthop List End
```

debug lacp

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

Synopsis **debug lacp** {**all** | **cli** | **event** | **ha** | **pdu** [**rx** {**all** | **interface tengigabitethernet** *rbridge-id/slot/port* | *interface gigabitethernet rbridge-id/slot/port*} | **tx** {**all** | **interface tengigabitethernet** *rbridge-id/slot/port* | *interface gigabitethernet rbridge-id/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.

ha Echo HA events to the console.

pdu Echo PDU content to the console.

- **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.
    - *rbridge-id* Specifies the ID of the routing bridge. This is not valid in standalone mode.
    - *slot* Specifies a valid slot number.
    - *port* Specifies a valid port number.
  - **interface gigabitethernet** Specifies a valid 1 Gbps Ethernet interface.
    - *rbridge-id* Specifies the ID of the routing bridge. This is not valid in standalone mode.
    - *slot* Specifies a valid slot number.
    - *port* Specifies a valid 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.
    - *rbridge-id* Specifies the ID of the routing bridge. This is not valid in standalone mode.
    - *slot* Specifies a valid slot number.
    - *port* Specifies a valid port number.
  - **interface gigabitethernet** Specifies a valid 1 Gbps Ethernet interface.
    - *rbridge-id* Specifies the ID of the routing bridge. This is not valid in standalone mode.
    - *slot* Specifies a valid slot number.

port	Specifies a valid port number.
sync	Echo synchronization to consoles.
timer	Echo timer expiration to console.
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** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/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.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	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.
	rx	Turns on detailed debugging for only received LLDP packets.
	tx	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 lldp 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* | **gigabitethernet** *slot/port*]}

no debug spanning-tree {**all** | **bpdu** [**rx** | **tx** [**all** | **interface port-channel** *number* | **tengigabitethernet** *slot/port* | **gigabitethernet** *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.
gigabitethernet	Specifies a valid 1 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# debug spanning-tree bpdu rx interface tengigabitethernet 0/1
switch# debug spanning-tree bpdu tx interface tengigabitethernet 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**

debug vrrp

Specifies debug settings.

Synopsis **debug vrrp all**

debug vrrp events

debug vrrp packets {interface {FortyGigabitEthernet *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **TenGigabitEthernet** *rbridge-id/slot/port*}**| recv | sent}**

debug vrrp session *VRID*

no debug vrrp all

no debug vrrp events

no debug vrrp packets {interface {FortyGigabitEthernet *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **TenGigabitEthernet** *rbridge-id/slot/port*}**| recv | sent}**

debug vrrp session *VRID*

Operands

all Debugs all VRRP events, packets, and sessions.

events Debugs all VRRP events.

packets interface Debugs packets for an interface that you specify. Also enables the *recv* and *sent* options.

FortyGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 40-Gbps port interface.

rbridge-id Specifies the ID of the routing bridge. This operand is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

GigabitEthernet *rbridge-id/slot/port*
Specifies a valid 1-Gbps Ethernet interface

rbridge-id Specifies the ID of the routing bridge.

slot Specifies a valid slot number.

port Specifies a valid port number.

TenGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 10-Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan#* Specifies the vlan number.

packets *recv* Debugs packets received.

packets *sent* Debugs packets sent.

session *VRID* Specifies the virtual group ID to debug. Range is 1 to 128.

Default None.

Command Modes Privileged EXEC mode.

Description Specifies the settings for capturing debugging information. You can, for example, capture event and packet information for all virtual groups or for a specific interface.

Usage Guidelines This command is for VRRP and VRRP-E. VRRP-E supports only the *ve* interface type. You can use the **no** parameter with the events and packets options to remove those configurations.

Examples To set debugging on sent and received packets for a TengGigabitEthernet interface that has an *rbridge-id/slot/port* of 121/0/50:

```
switch# debug vrrp packets interface tengigabitethernet 121/0/50
```

To set debugging for a session for a VRRP virtual group called *vrrp-group-25*:

```
switch# debug vrrp session 25
```

See Also vrrp-extended-group, vrrp-group

default-information-originate

Controls distribution of default information.

Synopsis **default-information-originate [always] [metric** *metric*] **[metric-type {type-1 | type-2}]**

Operands

always	**A**lways advertises the default route. If the route table manager does not have a default route, the router advertises the route as pointing to itself.
metric *metric*	Used for generating the default route, this option specifies the cost for reaching the rest of the world through this route. If you omit this option and do not specify a value using the *default-metric* router configuration command, a default metric value of 1 is used. The default is 10. The range is 1 to 65535.
metric-type	Specifies how the cost of a neighbor metric is determined. The default is type-1. However, this default can be changed with the **metric-type** command.
type-1	The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.
type-2	The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

Default Defaults for operands are listed above.

Command Modes Router configuration mode.

Description Notifies each OSPF router to redistribute any default routes found in the route table manager, whether static or learned from another protocol, to its neighbors.

Usage Guidelines Use the **no** parameter to disable this command.

Examples To always advertise the default route using a metric value of 20:

```
switch(conf-ospf-router)# default-information-originate always metric 20
```

See Also **default-metric, metric-type**

default-metric

Sets the default metric value for the OSPF routing protocol.

Synopsis **default-metric** *metric*

Operands

metric	Default metric value.

Default 10

Command Modes Router configuration mode.

Description A default metric overwrites any incompatible metrics that may exist when OSPF redistributes routes. Therefore, setting the default metric ensures that neighbors will use correct cost and router computation.

Usage Guidelines Use the **no** parameter to disable this configuration.

Examples To set the default metric to 20:

```
Switch(conf-ospf-router)# default-metric 20
```

See Also **default-information-originate**

delete

Deletes a file from the flash memory.

Synopsis **delete** *file*

Operands

file	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 user-generated copy of a configuration file:

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

switch# delete myconfig
% Warning: File will be deleted (from flash:)!
Continue?(y/n):y
```

See Also **copy, dir, rename, show file**

deny (extended ACLs)

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

Synopsis **deny** {**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [*EtherType* | **arp** | **fcoe** | **ipv4**] [**count**}

no deny {**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [*EtherType* | **arp** | **fcoe** | **ipv4**}

Operands

any	Specifies any source MAC address.
host *MAC_ADDRESS*	Specifies the source host MAC address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
MAC_ADDRESS	Specifies the destination host MAC address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
any	Specifies any destination MAC address.
host *MAC_ADDRESS*	Specifies the source host address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
MAC_ADDRESS	Specifies the destination host address for which to set deny conditions. Use the format HHHH.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 addresses 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_ADDRESS* | *MAC_ADDRESS*] parameters is specific to the source MAC address. The second set of [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] parameters is specific to the destination MAC address.

Examples To create a rule in a MAC extended address 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
```

To delete a rule from a MAC extended address:

```
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_ADDRESS* | **any**} [**count**]

no deny {*MAC_ADDRESS* | **any**}

Operands

MAC_ADDRESS	Specifies the source host MAC address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
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 None

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)

Describes the interface.

Synopsis **description** *line*

no description

Operands

line	Specifies characters describing the interface. The maximum number of characters is 63.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te, Ve).

Description Use this command to specify a string that contains the description of a specific interface.

Usage Guidelines Use the **no description** command to remove the description.

Examples To set the string describing internal tengigabitethernet interface 101/0/1:

```
switch(config)# interface tengigabitethernet 101/0/1
switch(conf-if-te-101/0/1)# description converged_101
```

See Also **interface**, **interface Ve**

description (LLDP)

Specifies a string that contains the description of LLDP.

Synopsis **description** *line*

no description

Operands *line* Characters describing LLDP. The maximum number of characters is 50.

Defaults None

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 None

Examples To set the strings describing LLDP:

```
switch(conf-lldp)# description Brocade-LLDP
```

See Also None

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:

```
switch(config)# monitor session 1
switch(config-mon-sess-1)# description server group 1 switch-cmsh
```

See Also **monitor session**

desire-distance

Sets the desired distance attribute for a Fibre Channel port used in the Dynamic (LD) or Static Long-Distance (LS) modes.

Synopsis **desire-distance** *distance*

Operands *distance* The length (in km) of the desired link.

Defaults The default value is 0.

Command Modes Interface Fibre Channel configuration submode.

Description For a Fibre Channel link configured with Static Long Distance (LS) mode, use this command to set the length of the desired long distance. The calculation of buffer-to-buffer credits is based on this length.

For a long distance Fibre Channel link configured with Dynamic mode (LD), use this command to set the maximum length to be used in calculating buffer-to-buffer credits. In this mode, the smaller of the distance measured during port initialization and the desired distance is used in the calculation.

Usage Guidelines This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples To set the desired distance Fibre Channel port attribute:

```
switch(config)# interface FibreChannel 7/0/2
switch(config-FibreChannel-7/0/2)# long-distance ls
switch(config-FibreChannel-7/0/2)# desire-distance 100
```

See Also **fill-word, interface, isl-r_rdy, long-distance, show running-config interface FibreChannel, shutdown, speed (Fibre Channel), trunk-enable, vc-link-init**

diag burninerrclear

Clears the error logs that are stored in the nonvolatile memory. These error logs are stored during POST and systemVerification failures. Error logs are automatically cleared during system verification.

Synopsis **diag burninerrclear**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear errors that are stored in the nonvolatile storage during the POST and system verification processes.

Usage Guidelines None

Examples

```
switch# diag burninerrclear
Clearing errLog for slot M2
Clearing errLog for slot S1
Clearing errLog for slot S2
Clearing errLog for slot S3
Clearing errLog for slot L4
```

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

diag clearerror

Clears the diagnostic errors encountered during offline diagnostic tests.

Synopsis **diag clearerror**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the diagnostics failure status.

Usage Guidelines This command is valid only on fixed-configuration switches.

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 LED tests and validates the functionality on a given slot-based switch or fixed-configuration switch.

CAUTION

This is a disruptive command. You must disable the switch and chassis before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

- During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.
- In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of cleanup.
- The rbridge-id is an optional parameter. If the rbridge-id is not specified, the test is assigned to the local rbridge-id.

Synopsis **diag portledtest** [**action** *pattern*] [**ethernet** *rbridgeid/slot/port*] [**fibrechannel** *rbridgeid/slot/port*] [**npass** *count*] [**slot** *slot_id*]

Operands

action *pattern*		Specifies the LED pattern. Action choices are as follows:
	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
ethernet		The logical Ethernet interface name, which is mutually exclusive from the Fibre Channel option. By default, all ports are tested.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number
fibrechannel		The logical Fibre Channel interface name, which is mutually exclusive from the Ethernet option. By default, all ports are tested.
	rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.
npass *count*		Specifies the number of times to perform this test. The default value is 1. The range of valid values is from 1 through 10.
slot *slot_id*		Specifies the slot identifiers for slot-based systems only.

Defaults By default, all the ports are tested in a switch. The default number of times to perform the test is 1.

The default **action** is cycle_all

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

Description Use this command to exercise the user port LEDs.

Usage Guidelines This test can be run on a single port or on all ports in the blade (slot-based switches) or the switch (fixed-configuration switches).

Examples The following commands allow you to run various action modes on the LEDs and validate the functionality.

In slot-based switches:

```
switch# diag portledtest action cycle-all slot L1

% Info: This test should be run to completion. Please do not abort while it is
executing.
Running portledtest...
Turning Port Status LEDs OFF...
Turning Port Status LEDs AMBER...
Turning Port Status LEDs GREEN...
Turning Port Status LEDs BLINK GREEN...
Turning Port Status LEDs BLINK AMBER...
portLedTest on slot L1 PASSED
% Info: Resetting the blade. Please wait till it gets initialized...
switch#
```

In fixed-configuration switches:

```
switch# diag portledtest
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running portledtest ...
Testing Ethernet ports..
STATUS LED OFF test
STATUS LED GREEN test
STATUS LED AMBER test
STATUS LED BLINK GREEN test
STATUS LED BLINK AMBER test
Testing FC ports..
STATUS LED OFF test
STATUS LED GREEN test
STATUS LED AMBER test
STATUS LED BLINK GREEN test
STATUS LED BLINK AMBER test
PASSED.
```

See Also **diag portloopbacktest, diag post enable, diag turboramtest**

diag portloopbacktest

Runs the port loopback test on a given slot-based switch or fixed-configuration switch. You can run this test on a single port or on all ports in the blade (slot-based switches) or switch (fixed-configuration switches). This functional test verifies the ability of each port to transmit and receive frames by setting up the loopback at various levels and speed modes.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

- During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.
- In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of cleanup.
- The rbridge-id is an optional parameter. If the rbridge-id is not specified, the test is assigned to the local rbridge-id.

Synopsis **diag portloopbacktest** [**ethernet** *rbridgeid/slot/port*] [**fibrechannel** *rbridgeid/slot/port*] [**lbmode** *loopback_mode*] [**nframes** *count*] [**slot** *slot_id*] [**spdmode** *mode*]

Operands

ethernet	The logical Ethernet interface name, which is mutually exclusive from the Fibre Channel option. By default, all ports are tested.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number
fibrechannel	The logical Fibre Channel interface name, which is mutually exclusive from the Ethernet option. By default, all ports are tested.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
lbmode *mode*	Specifies the loopback point for the test. Values are 1 (external) or 2 (internal) and the default is 2.
nframes *count*	Specifies the number of frames to send. The value range is from 1 through 16 and the default is 16.
slot *slot_id*	Specifies the slot identifiers for slot-based systems only.
spdmode *mode*	Specifies the speed mode for the test. This parameter controls the speed at which each port operates during the test. Valid options are as follows: – 1 Gbps – 2 Gbps – 4 Gbps

– 8 Gbps
– 10 Gbps
– 16 Gbps
– 40 Gbps

Defaults The default number of frames (**nframes**) is 16.

The default loopback mode (**lbmode**) 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)

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

Usage Guidelines None

Examples In slot-based switches:

```
switch# diag portloopbacktest slot S1
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running portloopbacktest...
<..cut..>
portLoopbackTest on ports 0-143 PASSED
portLoopbackTest on slot S1 PASSED
% Info: Resetting the blade. Please wait till it gets initialized...
```

In fixed-configuration switches:

```
switch# diag portloopbacktest
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running portloopbacktest ..............
PASSED.
```

See Also **diag portledtest, diag post enable, diag turboramtest**

diag post enable

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

Synopsis **diag post** [*rbridge-id*] **enable**

no diag post [*rbridge-id*] **enable**

Operands

rbridge-id	Specifies the Rbridge ID on which POST is run.
enable	Enables the power-on self-test on the specified switch.

Defaults By default, POST is enabled.

Command Modes Global configuration mode

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

Usage Guidelines Following the **diag post enable** command, update the startup-config by copying the running-config to the start-up config, which takes effect during reboot or a power cycle.

The **no** option disables the POST.

Examples To enable POST:

```
switch# config
Entering configuration mode terminal
switch(config)# diag post rbridge-id 1 enable
switch(config)# exit
switch# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue?
[y/n]: y
1970/01/01-09:09:49, [DCM-1101], 2086, M2, INFO, VDX8770-4, Copy running-config
to startup-config operation successful on this node.
```

To disable POST:

```
switch(config)# no diag post rbridge-id 1 enable
```

See Also **show running-config diag post**

diag prbstest

Runs the Pseudo Random Bit Sequence (PRBS) test on a given slot to verify the backend connections between the line card (LC) and switch fabric module (SFM). This test is not supported on fixed-configuration switches nor can it be run on a per-port basis.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of the cleanup process.

Synopsis **diag prbstest slot {L1 | L2 | S1 | S2 ..} pattern {PRBS7 | PRBS23 | PRBS31}**

Operands

slot *slot*	Specifies the slot ID. This test is applicable for slot-based systems only.
pattern *pattern*	Specifies the PRBS pattern. Valid values are PRBS7, PRBS23, and PRBS31. The default is PRBS7, which is the least stressful pattern, whereas PRBS31 is the most stressful pattern.

Defaults The default PRBS pattern is PRBS7.

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

Description Use this command to verify the backend connections between LC and SFM. This command also verifies the internal blade connections when executed in LC.

Usage Guidelines None

Examples In slot-based switches:

```
switch# diag prbstest slot L6 pattern PRBS7
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running prbstest...
Initializing ASICs & Ports...
Performing Link Training from L6 to S1
Performing Link Training from L6 to S2
Performing Link Training from L6 to S3
Performing Link Training from L6 to S4
Performing Link Training from L6 to S5
Performing Link Training from L6 to S6
slot S1 ASIC 0 Port 29 Tap0: 0x08 Tap1: 0x32 Tap2: 0x1e
<..cut..>
slot S6 ASIC 1 Port 15 Tap0: 0x08 Tap1: 0x33 Tap2: 0x20
Performing Link Testing from L6 to S1
Performing Link Testing from L6 to S2
Performing Link Testing from L6 to S3
Performing Link Testing from L6 to S4
```

```
Performing Link Testing from L6 to S5
Performing Link Testing from L6 to S6
prbsTest on slot L6 PASSED

%Info: Resetting the blade. Please wait till it gets initialized...
```

See Also **diag portledtest, diag portloopbacktest, diag turboramtest**

diag setcycle

Configures all the parameters required for the system verification test.

Synopsis **diag setcycle**

Operands **None**

Defaults If, after you enter the diag setcycle command, you respond with **yes** (see example, below), the following settings are the default values:

- *num_of_runs*—The value range for number of runs to complete is 1 through 25 and the default is 1.
- *min_lb_mode*—The value options for minimum loopback mode is 1 (external) or 2 (internal) and the default is 2. If set to 1, all the external user ports must be connected with small form-factor pluggable devices (SFPs) and loopback plugs.
- *pled_passes*—The value range for number of loops for the portLedTest is 1 through 10 and the default is 1.
- *tbr_passes*—The value range for number of loops for the turborRamTest is 1 through 10 and the default is 1. This option is not supported on fixed configuration switches.
- *plb_nframes*—The value range for number of frames for the portLoopbackTest is from 4 through 16 and the default is 16.

If you respond with **no**, the system prompts you for these values.

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples To change the value of num_of_runs parameter to 3:

```
switch# diag setcycle num_of_runs 3
Setting number_of_runs to 3.
Committing changes to configuration
```

In slot-based switches:

```
0 is not a valid number of passes. See sample below.
rontee128# diag setcycle num_of_runs 0
-------------------------------------^
syntax error: "0" is out of range.
switch# diag setcycle
Do you want use default values [Y/N]?     :y
DEFAULT - KEYWORD       : COMMENT
replacing 2 with default 1
 1      - number_of_runs        : number of passes of verify
 2      - min_lb_mode   : Limits -lb_mode of tests
VERIFY - label : Label for run start and stop messages
 1      - tbr_passes    : turboramtest number of passes
replacing 8 with default 16
 16     - plb_nframes   : portloopbacktest number of frames default speed
 1      - pled_passes   : portledtest number of passes
```

```
 1      - prbs_p7       : LC Backplane test with pattern PRBS7+
16     - cplb_nframes  : portloopbacktest in Core Blade number of frames
Committing changes to configuration

switch# diag setcycle
Do you want use default values [Y/N]?     :y
DEFAULT - KEYWORD       : COMMENT
 1      - number_of_runs        : number of passes of verify (0=infinite)
 2      - min_lb_mode   : Limits -lb_mode of tests
 0      - sof   : Enable stop testing on first fail
 VERIFY - label : Label for run start and stop messages
 1      - tbr_passes    : turboramtest number of passes
 16     - plb_nframes   : portloopbacktest number of frames default speed
 0      - plb5_nframes  : portloopbacktest (lb_mode 5) number of frames default
speed
 0      - plb7_nframes  : portloopbacktest (lb_mode 7) number of frames
 0      - pled_action   : portledtest action for glowing all led's
 1      - pled_passes   : portledtest number of passes
 1      - prbs_p7       : LC Backplane test with pattern PRBS7+
 0      - prbs_p23      : LC Backplane test with pattern PRBS23+
 0      - prbs_p31      : LC Backplane test with pattern PRBS31+
 0      - cprbs_p7      : SFM Backplane test with pattern PRBS7+
 0      - cprbs_p23     : SFM Backplane test with pattern PRBS23+
 0      - cprbs_p31     : SFM Backplane test with pattern PRBS31+
 16     - cplb_nframes  : portloopbacktest in Core Blade number of frames
 0      - cplb7_nframes : portloopbacktest in Core Blades (lb_mode 7) number of
frames
```

In fixed-configuration switches:

```
switch# diag setcycle
Do you want use default values [Y/N]? :y
DEFAULT - KEYWORD : COMMENT
replacing 3 with default 1
1 - number_of_runs : number of passes of verify (0=infinite)
2 - min_lb_mode : Limits -lb_mode of tests
1 - tbr_passes : turboramtest number of passes
16 - plb_nframes : portloopbacktest number of frames default speed
Committing changes to configuration
```

See Also show diag setcycle

diag systemverification

Runs a combination of various hardware diagnostic tests based on the parameters set using the **diag setcycle** command.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

- Error logs are cleared automatically during system verification.
- To check the current run status, enter the **show diag burninstatus** command.
- All errors are stored in the non-volatile memory. You can check the error status using the **show diag burninerrshow** command.
- During abnormal termination or when terminated by using the stop option, the system might be in unusable state. Perform a reload to reboot the chassis or switch to recover.
- In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of the cleanup process.

Synopsis **diag systemverification** [*short*] [*stop*]

Operands

short	Sets the burn-in parameters that control the number of frames to one for a quick run.
stop	Stops the current systemVerification run.

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)

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

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
% Info: This test should be run to completion. Please do not abort while it is
executing.
systemverification: burnin parameters.
CURRENT - KEYWORD : DEFAULT
1 - number_of_runs : 1
2 - min_lb_mode :    2
1 - tbr_passes :     1
16 - plb_nframes :  16
<..cut..>
```

See Also None

diag turboramtest

This test performs a series of low-level structural tests to determine the basic health of the PCI or PCIe bus and the memories inside the switch ASIC.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of the cleanup process.

Synopsis **diag turboramtest** [**passcnt** *count*] [**slot** *slot_id*}

Operands

passcnt *count*	Specifies the number of test repetitions. By default, the test runs once. The range of valid values is from 1 through 10.
slot *slot_id*	Specifies the slot ID. This is mandatory for slot-based systems only.

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

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

Description Use this command to run a memory test of the ASIC chips.

Usage Guidelines None

Examples In slot-based switches:

```
switch# diag turboramtest slot S2
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running turboramtest...
Initializing ASIC 0 for BIST
Initializing ASIC 1 for BIST
Initializing ASIC 2 for BIST
turboRamTest on ASIC 0 PASSED
turboRamTest on ASIC 1 PASSED
turboRamTest on ASIC 2 PASSED
turboRamTest on slot S2 PASSED
% Info: Resetting the blade. Please wait till it gets initialized...
completed.
```

In fixed-configuration switches:

```
switch# diag turboramtest
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running turboramtest ..............
PASSED.
```

2 diag turboramtest

See Also None

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         4096 Jan  1  1970 ..
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 myconfig.vcs
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x   1 root     sys           697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--   1 root     root         6800 Feb 13 00:37 startup-config
```

See Also **copy, delete, show file, rename**

distance

Configures an administrative distance value for OSPF routes.

Synopsis **distance {external | inter-area | intra-area }** *distance*

Operands

external	Sets the distance for routes learned by redistribution from other routing domains.
inter-area	Sets the distance for all routes from one area to another area.
intra-area	Sets the distance for all routes within an area.
distance	Administrative distance value assigned to OSPF routes. The default is 110. The range is 1 to 255.

Default The default administrative distance value for OSPF routes is 110.

Command Modes Router Configuration Mode

Description Specifies the administrative distance for different OSPF route types. You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPF intra-area route is always preferred over an OSPF inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

Usage Guidelines Use the **no** parameter to disable this configuration.

Examples To set the distance value for all external routes to 125:

```
Switch(conf-ospf-router)# distance external 125
```

distribute-list route-map

Configures a distribute list.

Synopsis **distribute-list route-map** *map* **in**

Operands

map	Name of route map.

Default None.

Command Modes Router configuration mode.

Description Configures a distribute list that can filter Link State Advertisements (LSAs) received from other OSPF routers before adding the corresponding routes to the routing table.

Usage Guidelines Use the **no** parameter to remove this distribute list.

Examples To create a distribute list using a route map named *filter1* that has already been configured:

```
switch(conf-ospf-router)# distribute-list route-map filter1 in
```

dns

Sets the domain name service (DNS) parameters. The DNS parameters are the domain name and the name server IP address for primary and secondary name servers.

Synopsis **ip dns domain-name** *domain-name*

no ip dns domain-name

ip dns name-server *ip_address_of_name_server*

no ip dns name-server

Operands *domain-name* The domain name for the primary and secondary name servers.

ip_address_of_name_server
The IP address of the primary and secondary name servers. The IP address can be in IPv4 or IPv6 format.

Defaults This command has no default values.

Command Modes Global configuration mode

Description Use this command to set the DNS domain name and name-server IP address.

Usage Guidelines You can enter only two name server IP addresses and only IPv4 is supported.

Name servers can be entered or removed one at a time. The newly-entered name server will append to the existing name server.

Examples

```
switch(config)# ip dns domain-name  brocade.com
switch(config)# ip dns name-server  10.70.20.1
switch(config)# ip dns name-server  10.70.20.10
switch(config)# do show run | begin ip dns

ip dns domain-name brocade.com
ip dns name-server 10.70.20.1
ip dns name-server 10.70.20.10
```

See Also None

dot1x authentication

Enables dot1x on a port.

Synopsis **dot1x authentication**

no dot1x authentication

Operands None

Defaults By default, dot1x authentication is disabled for a port.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description Use this command to enable dot1x on a specific port.

Usage Guidelines Use the **no dot1x authentication** command to disable dot1x on the port and remove the configuration from 802.1X management.

Examples To enable dot1x on a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x authentication
```

To disable dot1x on a specific fortygigabitethernet-interface port and remove the configuration from 802.1X management:

```
switch(config)# interface fortygigabitethernet 180/0/6
switch(conf-if-fo-180/0/6)# no dot1x authentication
```

See Also **interface**, **dot1x port-control**, **dot1x quiet-period**, **dot1x reauthentication**, **dot1x reauthMax**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

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 None

Examples To enable 802.1X authentication globally:

```
switch(config)# dot1x enable
```

See Also None

dot1x port-control

Controls port-state authorization.

Synopsis **dot1x port-control {auto | force-authorized | force-unauthorized}**

no dot1x port-control

Operands

auto	Enables authentication on a port. The controlled port is unauthorized until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized. This has the effect of activating authentication on an 802.1x-enabled interface.
forced-authorized	Forces a port to remain in an authorized state. This also allows connection from multiple clients.
force-unauthorized	Forces a port to remain in an unauthorized state.

Defaults The default port state is auto.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description Use this command to control the authorization of a port state.

Usage Guidelines Use the **no dot1x port-control** command to return to the default setting.

Examples To enable the port state to auto on a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x port-control auto
```

To enable the port state to force-authorized on a specific fortygigabitethernet-interface port:

```
switch(config)# interface fortygigabitethernet 180/0/1
switch(conf-if-fo-180/0/1)# dot1x port-control force-authorized
```

See Also **interface**, **dot1x authentication**, **dot1x quiet-period**, **dot1x reauthentication**, **dot1x reauthMax**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

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** *seconds*

no dot1x quiet-period

Operands

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 subconfiguration mode (fo, gi, te).

Description Use this command to set the time in seconds after which a switch attempts to perform authentication after a failed authentication. 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. Use the **no dot1x quiet-period** command to return to the default setting.

Examples To change the interval time to 200 seconds on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/9)# dot1x quiet-period 200
```

To set the interval time to the default value on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 180/0/6
switch(conf-if-fo-180/0/6)# no dot1x quiet-period
```

See Also **interface**, **dot1x authentication**, **dot1x port-control**, **dot1x reauthentication**, **dot1x reauthMax**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

dot1x reauthenticate interface

Initiates reauthentication on a specified interface.

Synopsis **dot1x reauthenticate interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines None

Examples To initiate reauthentication on interface tengigabitethernet 0/16:

```
switch#dot1x reauthenticate interface tengigabitethernet 0/16
```

See Also None

dot1x reauthentication

Enables port reauthentication.

Synopsis **dot1x reauthentication**

no dot1x reauthentication

Operands None

Defaults By default, reauthentication is disabled.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description Use this command to enable reauthentication on a port.

Usage Guidelines Use the **no dot1x reauthentication** command to return to the default settings.

Examples To enable reauthentication on a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x reauthentication
```

To disable reauthentication on a specific gigabitethernet-interface port:

```
switch(config)# interface gigabitethernet 178/2/9
switch(conf-if-gi-178/2/9)# no dot1x reauthentication
```

See Also **interface**, **dot1x authentication**, **dot1x port-control**, **dot1x quiet-period**, **dot1x reauthMax**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

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 subconfiguration mode (fo, gi, te).

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.

Usage Guidelines Use the **no dot1x reauthMax** command to return to the default setting.

Examples To set the maximum number of reauthentication attempts to 5 on a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x reauthMax 5
```

To set the reauthentication maximum to the default value on a specific fortygigabitethernet-interface port:

```
switch(config)# interface fortygigabitethernet 180/1/9
switch(conf-if-fo-180/1/9)# no dot1x reauthMax
```

See Also **interface**, **dot1x authentication**, **dot1x port-control**, **dot1x quiet-period**, **dot1x reauthentication**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

dot1x test eapol-capable

Executes the 802.1x readiness check on the switch.

Synopsis **dot1x test eapol-capable interface** [**gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*]

Operands

gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is designated as 802.1x-capable.

If you omit the optional interface keyword, all interfaces on the switch are tested. The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone).

Usage Guidelines The readiness check is not available on a port that is configured with the command **dot1x force-unauthorized**.

Examples The following is an example of configuring the readiness check:

```
switch# dot1x test eapol-capable interface tengigabitethernet 1/0/13
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on tengigabitethernet1/0/13
is EAPOL capable.
```

See Also None

dot1x test timeout

Sets the readiness test timeout.

Synopsis **dot1x test timeout** *timeout*

Operands

timeout	Specifies the interval value in seconds. The range of valid values is from 1 through 65535.

Defaults The default value is 10 seconds.

Command Modes Global configuration mode

Description Use this command to set the readiness test timeout.

Usage Guidelines None

Examples Example of setting the test timeout to 30 seconds:

```
switch(config)# dot1x test timeout 30
```

See Also **dot1x test eapol-capable**

dot1x timeout re-authperiod

Sets reauthorization-attempts interval.

Synopsis **dot1x timeout re-authperiod** *seconds*

no dot1x timeout re-authperiod

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 subconfiguration mode (fo, gi, te).

Description Use this command to set the number of seconds between reauthorization attempts on a specific interface.

Usage Guidelines Use **no dot1x timeout re-authperiod** to return to the default setting.

Examples To set 25 seconds as the amount of time between reauthorization attempts on a specific gigabitethernet interface:

```
switch(config)# interface gigabitethernet 190/0/9
switch(conf-if-gi-190/0/9)# dot1x timeout re-authperiod 25
```

To set the time between reauthorization attempts to the default value on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 180/0/5
switch(conf-if-fo-180/0/5)# no dot1x timeout re-authperiod
```

See Also **interface**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

dot1x timeout server-timeout

Sets authentication-sever response timeout.

Synopsis **dot1x timeout server-timeout** *seconds*

no dot1x timeout server-timeout

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 subconfiguration mode (fo, gi, te).

Description Use this command to set the authentication sever response timeout on a specific interface.

Usage Guidelines Use **no dot1x timeout server-timeout** to return to the default setting.

Examples To set 40 seconds as the switch-to-authentication server transmission time on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x timeout server-timeout 40
```

To set the switch-to-authentication server transmission time to the default value on a specific gigabitethernet interface:

```
switch(config)# interface gigabitethernet 170/4/2
switch(conf-if-gi-170/4/2)# no dot1x timeout server-timeout
```

See Also **interface**, **dot1x timeout re-authperiod**, **dot1x timeout supp-timeout**, **dot1x timeout tx-period**

dot1x timeout supp-timeout

Specifies the EAP response timeout.

Synopsis **dot1x timeout supp-timeout** *seconds*

no dot1x timeout supp-timeout

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 subconfiguration mode (fo, gi, te).

Description Use this command to 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.

Usage Guidelines Use **no dot1x timeout supp-timeout** to return to the default setting.

Examples To set 45 seconds as the switch-to-client retransmission time for the EAP request frame on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/8
switch(conf-if-te-178/0/8)# dot1x timeout supp-timeout 45
```

To set the switch-to-client retransmission time for the EAP request frame to the default value on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 190/0/16
switch(conf-if-fo-190/0/16)# no dot1x timeout supp-timeout
```

See Also **interface**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout tx-period**

dot1x timeout tx-period

Sets the time the switch waits for a response to an Extensible Authentication Protocol (EAP) request or identity frame.

Synopsis **dot1x timeout tx-period** *seconds*

no dot1x timeout tx-period

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 subconfiguration mode (fo, gi, te).

Description Use this command to set the interval (in seconds) between successive attempts to request an ID (EAP ID Req) or identity frame from the client.

Usage Guidelines Use **no dot1x timeout tx-period** to return to the default settings.

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 on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/16
switch(conf-if-te-190/0/16)# dot1x timeout tx-period 34
```

To set the interval between successive attempts to request an ID (EAP ID Req) to the default value on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 180/0/8
switch(conf-if-fo-180/0/8)# no dot1x timeout tx-period
```

See Also **interface**, **dot1x timeout re-authperiod**, **dot1x timeout server-timeout**, **dot1x timeout supp-timeout**

dpod

Manages Dynamic Ports on Demand (POD) assignments.

Synopsis **dpod** *rbridge-id/slot/port* {**reserve** | **release**}

Operands

rbridge-id	Specifies a switch by its RBridge identifier.
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 This command has no default values.

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.

This command has no effect on the Brocade VDX 6710 and on the Brocade VDX 8770. These platforms do not support ports on demand.

In the Network OS v3.0.0 release this command is supported only on the local switch.

Examples To reserve a POD assignment:

```
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 5/0/10 release
switch(config-dpod-5/0/10)# exit
switch(config)# dpod 5/0/11 release
switch(config-dpod-5/0/11)# exit
```

See Also **show dpod, show running-config dpod**

edge-loop-detection port-priority

Sets the ELD priority for a port.

Synopsis **edge-loop-detection port-priority** *eld-priority*

no edge-loop-detection port-priority

Operands

eld-priority	Specifies the port priority in the range from 0 through 256, where a higher number indicates a lower priority.

Defaults The ELD priority is set to 128.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to determine which of the ports involved in a loop will be disabled when the pdu-rx-limit for the Brocade VCS Fabric cluster is reached. The port with the lower priority (higher ELD-priority setting) is the port that is selected to be disabled.

If ELD must select between two ports with the same priority, ELD selects the port with the higher port ID to be disabled.

Usage Guidelines This command applies only in Brocade VCS Fabric mode.

Use the **no edge-loop-detection port-priority** command to restore the default ELD priority of 128.

You must use the **edge-loop-detection** command to enable edge-loop detection separately on the port for the ELD priority to be effective.

Examples To set the ELD priority of a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 5/0/10
switch(cfg-if-te-5/0/10)# edge-loop-detection port-priority 5
```

To restore the default ELD priority of 128 to a specific fortygigabitethernet-interface port:

```
switch(config)# interface fortygigabitethernet 8/1/12
switch(cfg-if-fo-8/1/12)# no edge-loop-detection port-priority
```

See Also **interface**, **clear edge-loop-detection**, **edge-loop-detection VLAN**, **hello-interval**, **pdu-rx-limit**, **show edge-loop-detection globals**, **show edge-loop-detection interface**, **show edge-loop-detection rbridge-id**, **shutdown-time**

edge-loop-detection VLAN

Enables edge-loop detection on a port and VLAN.

Synopsis **edge-loop-detection VLAN** *vlan-ID*

no edge-loop-detection VLAN *vlan-ID*

Operands

VLAN *vlan-id*	Specifies the VLAN interface number in the range of 1 to 4090 on the selected port.

Defaults Edge-loop detection is disabled.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use the VLAN operand to specify a VLAN and port on which to enable edge-loop detection. The port must be a member of the specified VLAN or the command returns an error.

Usage Guidelines This command applies to Brocade VCS Fabric mode only.

This functionality detects Layer 2 loops only.

Use the **no edge-loop-detection VLAN** *vlan-ID* command to disable edge-loop detection on the port and VLAN.

Examples To enable edge-loop detection on VLAN 10 for a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 1/0/7
switch(conf-if-te-1/0/7)# edge-loop-detection vlan 10
```

To **disable edge-loop detection on a specific gigabitethernet port and a VLAN** whose ID is 20:

```
switch(config)# interface gigabitethernet 170/1/9
switch(conf-if-gi-170/1/9)# no edge-loop-detection vlan 20
```

See Also **interface**, **clear edge-loop-detection**, **edge-loop-detection port-priority**, **hello-interval**, **show edge-loop-detection globals**, **shutdown-time**

end

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

Synopsis **end**

Operands None

Defaults None

Command Modes All configuration modes

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

Usage Guidelines None

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
```

See Also interface, 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 None

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.

This command does not function in VCS mode.

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

Sets the timeout for errors on an interface.

Synopsis **error-disable-timeout interval** *seconds*

no error-disable-timeout interval

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 Use the **no error-disable-timeout interval** command to reset the value to the default.

This command does not function in VCS mode.

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 None

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 None

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

```
switch(config)#interface tengigabitethernet 0/1
switch(conf-if-te-0/1)#exit
switch(config)#exit
```

See Also **interface**, **end**

external-lsdb-limit

Configures the maximum size of the external link state database (LSDB).

Synopsis **external-lsdb-limit** *value*

Operands

value	Maximum size of the external LSDB. The maximum allowed value is 14913080.

Default 14913080

Command Modes Router configuration mode.

Description Configures the maximum size of the external LSDB. If you change the value, make sure to save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

Usage Guidelines Use the **no** parameter to reset the maximum number of entries to its system default.

Examples To set the limit of the LSDB to 20000:

```
switch(conf-ospf-router)# external-lsdb-limit 20000
```

See Also database-overflow-interval

fabric ecmp load-balance

Configures the hashing fields.

Synopsis **fabric ecmp load-balance** [**dst-mac-vid** | **src-dst-ip** | **src-dst-ip-mac-vid** | **src-dst-ip-mac-vid-port** | **src-dst-ip-port** | **src-dst-mac-vid** | **src-mac-vid**]

Operands

dst-mac-vid	Configures the command to use destination MAC address and VID based load balancing.
src-dst-ip	Configures the command to use source and destination IP address based load balancing.
src-dst-ip-mac-vid	Configures the command to use source and destination IP and MAC address and VID based load balancing.
src-dst-ip-mac-vid-port	Configures the command to use source and destination IP, MAC address, VID and TCP/UDP port based load balancing.
src-dst-ip-port	Configures the command to use source and destination IP and TCP/UDP port based load balancing.
src-dst-mac-vid	Configures the command to use source and destination MAC address and VID based load balancing.
src-mac-vid	Configures the command to use source MAC address and VID based load balancing.

Defaults None

Command Modes Rbridge ID configuration mode

Description This command configures the list of fields (in the incoming packets), used for hashing.

Usage Guidelines This command does not function in standalone mode.

Examples Example of setting the ECMP load balance to use source and destination IP address based load balancing:

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# fabric ecmp load-balance src-dst-ip
```

See Also **fabric ecmp load-balance-hash-swap**

fabric ecmp load-balance-hash-swap

Configures how to swap the input fields before feeding them to the hash function.

Synopsis **fabric ecmp load-balance-hash-swap** *value*

Operands

value	The control value. The range of valid values is from 0x0 through 0xFFFFFFFF.

Defaults None

Command Modes Rbridge ID configuration mode

Description This command is used to configure how to swap the input fields before feeding them to the hash function. The variable value for this command is interpreted as the bitwise control of the 212-bit key. Each bit controls whether 2 adjacent bits of the key are to be swapped. This 32-bit control value is written to all four hash swap control registers. This means that this value is replicated in a 32-bit block to form a 106-bit value. A value of 0x0 does not swap any input fields, while a value of 0xffffffff swaps all 106 input bit-pairs.

Usage Guidelines This command does not function in standalone mode.

Examples None

See Also **fabric ecmp load-balance**

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

Defaults By default, ISL ports are enabled persistently.

Command Modes Interface subconfiguration mode (fo, te).

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.

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

This command functions in Brocade VCS Fabric mode only.

Use the **no fabric isl enable command to disable** the administration and operational state of an inter-switch link (ISL).

Examples To enable the administration and operational state of an ISL on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 1/0/18
switch(config-if-te-1/0/18)# fabric isl enable
```

To disable the administration and operational state of an ISL on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/1/15
switch(config-if-fo-1/1/15)# no fabric isl enable
```

See Also **interface**, **diag setcycle, show diag burninstatus, vcs, fabric trunk enable**

fabric route mcast

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

Synopsis **fabric route mcast rbridge-id** *rbridge-id* **priority** *priority*

Operands

rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
rbridge-id	Specifies the RBridge identifier.
priority	Sets a priority (default is 1). The highest priority overrides the lowest RBridge ID and becomes the root.
priority	Specifies the priority number of the RBridge.

Defaults The default priority is 1.

Command Modes Global configuration mode

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.

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

This command is not valid in standalone mode.

Examples To change an RBridge multicast priority:

```
switch(config)# fabric route mcast rbridge-id 45 priority 5
switch(config)# exit
switch# show running-config fabric route mcast rbridge-id 45 priority
fabric route mcast rbridge-id 45 priority 5
```

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

Defaults Fabric trunking is enabled by default.

Command Modes Interface subconfiguration mode (fo, te)

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.

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

This command functions in Brocade VCS Fabric mode only.

Use the **no fabric trunk enable** command to disable trunking on a port.

Examples To enable a port for trunking on a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 1/0/18
switch(config-if-te-1/0/18)# fabric trunk enable
```

To disable a port for trunking on a specific fortygigabitethernet-interface port:

```
switch(config)# interface fortygigabitethernet 8/10/15
switch(config-if-fo-8/10/15)# no fabric trunk enable
```

See Also **interface**, **show fabric trunk, fabric isl enable**

fabric vlag

Configures the load balancing feature on a remote Rbridge.

Synopsis **fabric vlag** *port-channel-id* **load-balance** *flavor*

Operands

port-channel-id	The port channel ID.
load-balance *flavor*	The flavor to assign to the remote Rbridge. See Table 1.

Defaults The default value is src-dst-ip-mac-vid-port.

Command Modes RBridge configuration mode

Description This feature allows you to configure the load balancing feature on a remote Rbridge which is not a member of the vLAG (also known as a non-local RBridge), to forward traffic to a vLAG. To distribute the traffic among the possible paths towards the VLAG, you can configure the vlag-load-balancing flavor on RB2. Available flavors are listed in Table 1.

TABLE 1 Load balance flavors

dst-mac-vid	Destination MAC address and VID based load balancing.
src-mac-vid	Source MAC address and VID based load balancing.
src-dst-mac-vid	Source and Destination MAC address and VID based load balancing.
src-dst-ip	Source and Destination IP address based load balancing.
src-dst-ip-mac-vid	Source and Destination IP and MAC address and VID based load balancing.
src-dst-ip-port	Source and Destination IP and TCP/UDP port based load balancing.
src-dst-ip-mac-vid-port	Source and Destination IP, MAC address, VID and TCP/UDP port based load balancing.

Additionally, an Rbridge can be set to a different flavor for different vLAGs present in the cluster. This feature is available for each Rbridge and each VLAG, so different load-balance flavors can be set for traffic directed towards different VLAGs.

Usage Guidelines None

Examples

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# fabric vlag 20 load-balance dst-mac-vid
switch(config-rbridge-id-2)# end
```

See Also None

fabric-map

Enables the Fabric-Map sub-mode.

Synopsis **fabric-map default**

Operands None

Defaults None

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.

This command does not function in standalone mode.

Examples

```
switch(config)#fcoe
switch(config-fcoe)#fabric-map default
switch(config-fcoe-fabric-map)#
```

See Also **fcoe**

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, bypassing POST when the system comes back up. Bypassing POST can reduce boot time significantly.

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.

On a modular chassis, the **fastboot** commands only reboots the management module on which the command is executed. If you log in to the switch IP address and execute the fastboot command, only the active management module reboots and POST is bypassed.

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.

This command does not function in standalone mode.

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

fcoe

Enables the FCoE configuration mode.

Synopsis **fcoe**

Operands None

Defaults None

Command Modes Global configuration mode

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

Usage Guidelines None

Examples

```
switch(config)# fcoe
switch(config-fcoe)#
```

See Also **fcoe, fabric-map**

fcoe-profile (AMPP)

Activates the FCoE profile configuration mode.

Synopsis **fcoe-profile**

Operands None

Defaults None

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 The only fcoe-profile name allowed is “default”.

Examples

```
switch(config)# port-profile default
switch(conf-pp)# fcoe-profile
```

See Also None

fcoeport

Provisions a port with the default FCoE map.

Synopsis **fcoeport** *map*

no fcoeport

Operands *map* This must be **default**.

Defaults None

Command Modes Interface subconfiguration mode (Port-channel, te).

Description This command configures a specific port to be an FCoE port, with the assigned map name **default**.

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

Use the **no fcoeport** command to remove the FCoE port configuration from the applicable port.

Examples To provision a specific tengigabitethernet-interface port with the default FCoE map:

```
switch(config)# interface tengigabitethernet 101/0/1
switch(conf-if-te-101/0/1)# fcoeport default
```

See Also **interface**

fcsp auth

Configures the protocol specific parameters.

Synopsis **fcsp auth auth-type dh-chap group** {**0** | **1** | **2** | **3** | **4** | *****} **hash** {**sha1** | **md5** | **all**} **policy switch** {**on** | **off** | **active** | **passive**]}

Operands

auth-type dh-chap	Authentication type is DH-CHAP.
group	Specifies the DH group value. This parameter sets the strength of the secret. Values are 0, 1, 2, 3, 4 or *. The asterisk (*) indicates all values (0 through 4). The default value is *.
hash	Specifies the hash type used for authentication. Possible values are **sha1**, **md5**, or **all** (sha1 and md5). The default option is **all**.
policy switch	Configures the switch authentication policy attribute. Values are **on**, **off**, **passive**, or **active**. The default switch policy is **passive**.

Defaults None

Command Modes Global configuration mode

Description Use this command to configure the authentication policy attributes and controls its behavior. The policy configuration includes protocol specific parameters such as authentication type, DH-group value, and hash type. It also defines whether the policy is enabled or disabled and how strictly it is enforced.

Usage Guidelines The authentication policy can be set to any of these values:

- **ON** — Strict authentication is enforced on all E-ports. The ISL goes down (port disable) if the connecting switch does not support the authentication or the policy is OFF. During switch initialization, authentication is initiated on all E-ports automatically. The authentication is initiated automatically during the E-port bring-up by fabric module. The authentication handshaking is completed before the switches exchange the fabric parameters (EFP) for E-port bring-up.
- **ACTIVE** — In this policy, the switch is more tolerant and can be connected to a switch with any type of policy. During switch initialization, authentication is initiated on all E-ports, but the port is not disabled if the connecting switch does not support authentication or the authentication policy is OFF. The authentication is initiated automatically during the E_Port bring-up.
- **PASSIVE** (default) — The switch does not initiate authentication, but participates in authentication if the connecting switch initiates authentication. The switch does not start authentication on E_Ports, but accepts the incoming authentication requests, and will not disable if the connecting switch does not support authentication or the policy is OFF.
- **OFF** — The switch does not support authentication and rejects any authentication negotiation request from neighbor switch. A switch with the policy OFF should not be connected to a switch with policy ON, since the ON policy is strict and disables the port if any switch rejects the authentication. DH-CHAP shared secrets should be configured before switching on the policy from OFF state.

Once the authentication negotiation succeeds, the DH-CHAP authentication is initiated. If DH-CHAP authentication fails the port is disabled, This behavior applies to all modes of the policy.

Examples To configure the authentication type:.

```
switch(config)# fcsp auth auth-type dh-chap
```

To set only the hash type:

```
switch(config)# fcsp auth auth-type hash md5
```

To activate the device authentication policy:

```
switch(config)# fcsp auth policy switch active
```

See Also fcsp auth-secret, show fcsp auth-secret dh-chap, show running-config fcsp auth

fcsp auth-secret

Sets the shared secret for DH CHAP authentication.

Synopsis **fcsp auth-secret dhchap node** *switch_wwn* **peer-secret** *secret_key* **local-secret** *secret_key*

no fcsp auth-secret dhchap node *switch_wwn*

Operands **node** *switch_wwn* Specifies the world wide name (WWN) of the peer.

peer-secret *secret_key* Specifies the secret of the peer that authenticates the peer to the local switch.

local-secret *secret_key* Specifies the local secret that authenticates the local switch to the peer.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to set the shared secret for DH-CHAP authentication. The **no fcsp auth-secret dh-chap node** *switch_wwnn* removes the dh-chap authentication secrets from the data base, so that the switch with the given WWN cannot connect to the local switch.

Usage Guidelines The local and peer secret keys must be between 8 and 40 characters long.

Only the following non-alphanumeric characters are valid for the secret key:

@ $ % ^ & * ( ) _ + - < > { } [ ] ; ' :

This command is supported only on the Brocade VDX 6730 platforms.

Examples To set the shared secret for DH-CHAP authentication:

```
switch# fcsp auth-secret dhchap node 50:00:51:ed:2d:c0:1e:64 \peer-secret
12345678 local-secret 87654321
```

To remove the DH-CHAP authentication secrets from the database:

```
switch# fcsp auth-secret dhchap node 50:00:51:ed:2d:c0:1e:64
Shared secret successfully removed
```

See Also **fcsp auth, show fcsp auth-secret dh-chap, show running-config fcsp auth**

fill-word

Configures the link initialization and fill word primitives for an 8-GB Fibre Channel port.

Synopsis **fill-word** {**idle-idle** | **arbff-arbff** | **idle-arbff** | **aa-then-ia**}

Operands

idle-idle	Sets IDLE mode for the link initialization and IDLE as the fill word.
arbff-arbff	Sets ARB(ff) for the link initialization and ARB(ff) as the fill word,
idle-arbff	Sets IDLE mode for the link initialization and ARB(ff) as the fill word,
aa-then-ia	Attempts **arbff-arbff** first. If the attempt fails, goes into **idle-arbff** mode. The **aa-then-ia** mode is preferable as it captures more cases.

Defaults The default value is **idle-idle**.

Command Modes Interface Fibre Channel configuration submode

Description Use this command to configure the link initialization and fill word for an 8-GB Fibre Channel port. By default, this command disables and re-enables the port and the port comes online with the new fill word setting.

This command should be left at the default setting unless the remote port requires a specific setting for fill word.

Usage Guidelines This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples To set the fill word Fibre Channel port attribute:

```
switch(config)# interface FibreChannel 7/0/2
switch(config-FibreChannel-7/0/2)# fill-word arbff-arbff
```

See Also **desire-distance, interface, isl-r_rdy, long-distance, show running-config interface FibreChannel, shutdown, speed (Fibre Channel), trunk-enable, vc-link-init**

fips root disable

Permanently disables root access to a switch for compliance with Federal Information Processing Standards (FIPS).

Synopsis **fips root disable**

Operands None

Defaults By default, root access is enabled.

Command Modes Privileged EXEC mode

Description Use this command to disable root access to a switch permanently when preparing the switch for FIPS compliance. See the *Network OS Administrator's Guide* for details about preparing a switch for FIPS compliance.

Usage Guidelines Under normal operation, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "**fibranne**" to make the command available.

This command applies only in the standalone mode. It can be issued only from a user account with the admin role assigned.

CAUTION

Once root access is disabled, it cannot be re-enabled.

Examples To disable root access to a switch:

```
switch# unhide fips
Password: *****
switch# fips root disable
This operation disables root account. Do you want to continue? [yes,NO] yes
```

See Also **cipherset, fips selftests, fips zeroize, prom-access disable, show prom-access, unhide fips**

fips selftests

Enables Federal Information Processing Standards (FIPS) self tests which will be performed when the switch boots. If the tests run successfully, the switch comes up in the FIPS compliant state.

Synopsis **fips selftests**

Operands None

Defaults By default, the switch operates in the non-FIPS compliant state.

Command Modes Privileged EXEC mode

Description Use this command to enable FIPS self tests on the switch. These self tests include known answer tests (KATs) that exercise various features of FIPS algorithms and conditional tests that test the randomness of random number generators and check for signed firmware. These tests run when the switch boots. Successful completion of these tests places the switch into the FIPS compliant state. If any test returns an error, the switch reboots and runs the tests again. Whether tests succeed or fail, you cannot return the switch to the non-FIPS compliant state.

You typically use this command after disabling non-FIPS compliant features on the switch and configuring secure ciphers, but before zeroizing the switch with the **fips zeroize** command. These non-FIPS compliant features that must be disabled include Brocade VCS Fabric mode, the Boot PROM, root access, TACACS+ authentication, and the dot1x feature. Secure ciphers that must be configured are for the SSH protocol and (optionally) for the Lightweight Directory Access Protocol (LDAP) protocol. The **fips zeroize** command erases all critical security parameters and reboots the switch. See the *Network OS Administrator's Guide* for details about preparing a switch for FIPS compliance.

Usage Guidelines Under normal operation, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "**fibranne**" to make the command available.

This command applies only in the standalone mode. It can be entered only from a user account with the admin role assigned.

CAUTION

This command should be used only by qualified personnel. Once a switch is in the FIPS compliant state, you cannot return it to the non-FIPS compliant state.

Examples To enable the FIPS self tests:

```
switch# unhide fips
Password: *****
switch# fips selftests
Self tests enabled
```

See Also **fips root disable, fips zeroize, prom-access disable, show prom-access, unhide fips**

fips zeroize

Removes all critical security parameters from a switch in readiness for compliance with Federal Information Processing Standards (FIPS) and reboots the switch.

Synopsis **fips zeroize**

Operands None

Defaults By default, the switch operates in the non-FIPS compliant state.

Command Modes Privileged EXEC mode

Description Use this command to erase all critical security parameters from the switch in readiness for FIPS compliance including passwords, shared secrets, and private keys. This command also reboots the switch. If FIPS self tests are enabled and they run successfully during reboot, then the switch comes up in the FIPS compliant mode. If the FIPS self tests return errors, the switch reboots and runs the tests again.

Typical use of this command is after disabling non-FIPs compliant features, configuring secure ciphers, and enabling FIPS self tests with the **fips selftests** command. These non-FIPS compliant features that must be disabled include Brocade VCS Fabric mode, the Boot PROM, root access, TACACS+ authentication, and the dot1x feature. Secure ciphers that must be configured are for the SSH protocol and (optionally) for the Lightweight Directory Access Protocol (LDAP) protocol. See the *Network OS Administrator's Guide* for details about preparing a switch for FIPS compliance.

Usage Guidelines Under normal operation, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "**fibranne**" to make the command available.

This command applies only in the standalone mode. This command can be entered only from a user account with the admin role assigned.

CAUTION

This command should be used only by qualified personnel. Once a switch is in the FIPs compliant state, you cannot return it to the non-FIPS compliant state.

Examples To erase all critical security parameters from a switch:

```
switch# unhide fips
Password: *****
switch(config)# fips zeroize
This operation erases all passwords, shared secrets, private keys etc. on the
switch. Do you want to continue? [yes,NO] yes
```

See Also **fips selftests, fips root disable, prom-access disable, show prom-access, unhide fips**

firmware commit

Commits a firmware upgrade.

Synopsis **firmware commit**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to copy the firmware image from the primary partition to the secondary partition. This command is effective only after a firmware download (with auto-commit mode disabled) and a reboot.

Usage Guidelines **The firmware download command** updates the secondary partitions only. When the **firmware download** command completes successfully and the switch reboots, the system swaps partitions. The primary partition (with the previous 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 disable auto-commit 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.
- **firmware restore** – Copies the secondary partition (with the previous firmware) to the primary partition and restores the original firmware version.

This command is supported only on the local management modules.

You must run the **firmware download** command 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, show version**

firmware download

Downloads the firmware on the local switch.

Synopsis

firmware download interactive

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

firmware download usb directory *directory* [**manual**] [**nocommit**] [**noreboot**]

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.
manual	Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This option is ignored when issued on a compact switch or in a chassis with only one management module.
nocommit	Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.
noreboot	Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the switch comes back up.
host	Specifies the host by DNS name or IP address.
hostname	Specifies an IPv4 DNS host name.
host_ip_address	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
user *username*	Specifies the user login name for the host.
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 an auto-reboot and a subsequent auto-commit operation.

Command Modes Privileged EXEC mode

Description Use this command to download 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 device components supported by this command 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 firmware upgrades on the local switch only.

This command does not support pagination.

If the **firmware download** is interrupted because of 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 perform a firmware download in interactive mode using default options:

```
switch# firmware download interactive
firmware download interactive
Server name or IP address: 10.31.2.25
File name: /users/home40/Builds/NOS_v3.0.0
Protocol (ftp, scp): ftp
User: fvt
Password: **********
Do manual download [y/n]: n

System sanity check passed.

Do you want to continue? [y/n]: y
```

To perform a manual firmware download to a single management module:

```
switch# firmware download interactive
Server name or IP address: 10.31.2.25
File name: /users/home40/dist/NOSv3.0.0
Protocol (ftp, scp): ftp
User: admin
Password: **********
Do manual download [y/n]: y
Reboot system after download? [y/n]: y
Do Auto-Commit after Reboot? [y/n]: y
System sanity check passed.

You are running a firmware download on dual MM system with 'manual' option. This
will upgrade the firmware only on the local MM.

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
[output truncated]
```

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

```
switch# firmware download usb directory NOS_v3.0.0
```

To upgrade firmware using the command line:

```
switch# firmware download ftp host fe80::200:f8ff:fe21:67cf user admin
password  <password> directory /home/firmware/dist/nosv3.0.0t

System sanity check passed.
You are running running firmware download on dual MM system with 'manual' option.
This will upgrade the firmware only on the local MM. 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
```

See Also firmware commit, firmware restore, firmware sync, show firmwaredownloadstatus, 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 previously active firmware image. You can run this command only if auto-commit mode was disabled during the firmware download. After a firmware download and a reboot (with auto-commit mode disabled), the downloaded firmware becomes active. If you do not want to commit the firmware, use the **firmware restore** command.

This command reboots the system and reactivates the previous firmware. After reboot, all primary and secondary partitions restore the previous firmware image.

Usage Guidelines This command is supported only on the local management module.

The **firmware download** command must have been run with the **nocommit** option for the **firmware restore** operation to succeed.

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 **firmware commit, firmware download, firmware sync, show version**

firmware sync

Copies the firmware from the active to the standby management module.

Synopsis **firmware sync**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to copy the firmware from the active management module to the standby management module. This operation involves rebooting the management module.

Usage Guidelines This command makes a best effort to synchronize the management modules.

This command is not supported on the standby management module.

After completing the operation, use the **show version** command with the **all-partitions** option to verify that both management modules are running the same firmware version.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To synchronize the management modules on a Brocade VDX 8770 chassis:

```
switch# firmware sync
This command will approximately take 15 minutes to complete
Do you want to continue? [y/n]: y
2011/12/16-23:50:15, [EM-1049], 200, MM1, INFO, chassis, FRU MM2 insertion
detected.
2011/12/16-23:51:10, [EM-1047], 201, MM1, INFO, chassis, MM in slot 2 not faulty,
MM ERROR deasserted.
2011/12/16-23:51:43, [HASM-1104], 204, MM1, INFO, chassis, Heartbeat to MM2 up
2011/12/16-23:51:44, [SULB-1105], 205, MM1, INFO, chassis, Firmware upgrade
session (0: firmware sync (active -> standby)) starts.
2011/12/16-23:51:44, [SULB-1100], 206, MM1, INFO, chassis, Firmware install
begins on MM2.
2011/12/16-23:51:45, [HASM-1104], 209, MM2, INFO, chassis, Heartbeat to MM1 up
2011/12/16-23:55:26, [SULB-1101], 211, MM1, INFO, chassis, Firmware install ends
on MM2.
2011/12/16-23:55:29, [SULB-1100], 212, MM1, INFO, chassis, Firmware reboot begins
on MM2.
2011/12/16-23:55:37, [HASM-1102], 214, MM1, INFO, chassis, Heartbeat misses to
MM2 reached threshold.
2011/12/16-23:55:39, [HASM-1106], 215, MM1, INFO, chassis, Reset the standby
2011/12/16-23:57:33, [HASM-1104], 220, MM1, INFO, chassis, Heartbeat to MM2 up
2011/12/16-23:57:36, [HASM-1104], 223, MM2, INFO, chassis, Heartbeat to MM1 up
```

See Also **firmware commit, firmware download, show version**

forward-delay

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

Synopsis **forward-delay** *seconds* [**vlan** *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 *vlan_id*	Specifies the VLAN ID. Refer to "Description" below.

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.

If the VLAN parameter is not provided, the delay value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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)

Spanning tree commands do not function under Brocade VCS Fabric mode.

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

```
switch(conf-mstp)# forward-delay 18
```

See Also hello-time, max-age

ha chassisreboot

Performs a reboot of the chassis.

Synopsis **ha chassisreboot**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to perform a reboot of the entire chassis. Bothe the active and the standby management module reboot. Both management modules retain their original high-availability (HA) role after the system comes back up. If the power-on self test (POST) is enabled, it is executed when the system comes back up.

Usage Guidelines HA is not supported in this release. All failover and reboots are disruptive. The HA commands are provided for consistency and future expansion.

This command is supported only on the active management module.

This command is not supported on the standby management module.

Both management modules must be in sync for the HA reboot operation to succeed.

Examples To perform a HA reboot:

```
switch# ha chassisreboot
```

See Also **ha disable, ha enable, ha failover, show ha**

ha disable

Disables the High Availability feature.

Synopsis **ha disable**

Operands None

Defaults HA is by default disabled.

Command Modes Privileged EXEC mode

Description Use this command to disable the High Availability (HA) feature on a switch. If the HA feature is already disabled, this command has no effect.

Usage Guidelines HA is not supported in this release. All failover is disruptive. The HA commands are provided for consistency and future expansion.

This command is supported only on the active management module.

This command is not supported on the standby management module.

Examples To display the syslog daemon IP addresses configured on a switch:

```
switch# ha disable
Service instances out of sync
1970/01/01-00:06:30, [HASM-1101], 111, MM1, WARNING, chassis, HA State out of
sync.
HA is disabled
```

See Also **ha enable, ha failover, show ha**

ha dump

Displays High Availability status information.

Synopsis **ha dump**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the status of the High Availability (HA) feature on a chassis.

Usage Guidelines HA is not supported in this release. All failover is disruptive. The HA commands are provided for consistency and future expansion.

This command is for debugging purposes only.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples To display HA status:

```
switch# ha dump
```

See Also **ha disable, ha enable, ha failover, show ha**

ha enable

Enables the High Availability feature.

Synopsis **ha enable**

Operands None

Defaults HA is by default disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable the High Availability (HA) feature on a switch. If the HA feature is already enabled, this command has no effect.

If the HA feature is disabled, this command enables it. The standby management process reboots as part of the process.

The command displays a warning message and prompts for confirmation before rebooting the management module. 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 HA is not supported in this release. All failover is disruptive. The HA commands are provided for consistency and future expansion.

This command is supported only on the local management module.

This command is not supported on the standby management module.

Examples To display the syslog daemon IP addresses configured on a switch:

```
switch# ha enable

Warning: This command will enable the HA. It will reboot the standby CP and
require all telnet, secure telnet, and SSH sessions to the standby CP to be
restarted.

Are you sure you want to go ahead  [y/n]? y

1970/01/01-00:07:18, [EM-1047], 113, MM1, INFO, chassis, CP in slot 2 not faulty,
CP ERROR deasserted.
HTBT hit a threshold: 2
HTBT hit a threshold: 2
Heartbeat to 2 Down!
     resetting peer
     resetting peer 127.2.1.2
HA is enabled
```

See Also **ha disable, ha failover, show ha**

ha failover

Initiates a failover from the active to the standby management module.

Synopsis **ha failover**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to force a failover from the active to the standby management model. When the process completes, the former standby takes over as the active management module. If the active and standby management modules are not synchronized, the command aborts.

Usage Guidelines HA is not supported in this release. All failover is disruptive. The commands are provided for consistency and future expansion.

This command is supported only on the active management module.

Examples To perform a failover:

```
switch# ha failover
```

See Also **ha disable, ha enable**

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 None

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

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

See Also None

hello-interval

Sets the interval between PDU packets sent from the ELD-enabled edge ports of a Brocade VCS Fabric cluster.

Synopsis **hello-interval** *interval*

no hello-interval *interval*

Operands

interval	Number of ms periods between each PDU. For example, a value of 2000 causes a PDU to be sent every two seconds. The valid range is 100 through 5000 (100ms through 5 seconds).

Defaults 1000 (one second)

Command Modes ELD configuration mode

Description Use this command with the **pdu-rx-limit** command to determine the time taken to detect a loop. The time taken to detect a loop is the product of the pdu-rx-limit and the hello interval.

The hello interval must be set to the same value on all Brocade VCS Fabric clusters that have ELD enabled, otherwise it cannot be predicted which Brocade VCS Fabric cluster will reach its limit first. The Brocade VCS Fabric cluster in the loop with the lowest pdu-rx-limit is the cluster where the loop gets broken, assuming that the hello interval is correctly set to the same value on all clusters.

Usage Guidelines This command applies only in Brocade VCS Fabric mode.

This functionality detects Layer 2 loops only.

Use extreme caution when setting the hello interval value to less than 1 second because it heavily increases the CPU load due to the number of packets transmitted and received. This load depends on the number of ELD instances and other system configuration parameters. Undesirable performance and scalability might occur.

Examples To set the PDU interval to 5 seconds:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# hello-interval 5000
```

To reset the PDU interval to its default value of 1 second:

```
switch(cfg-eld)# no hello-interval 5000
```

See Also **pdu-rx-limit, protocol edge-loop-detection, show edge-loop-detection globals**

hello-time

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

Synopsis **hello-time** *seconds* [**vlan** *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 *vlan_id*	Specifies the VLAN ID. Refer to "Description" below.

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.

If the VLAN parameter is not provided, the hello-time value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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)

Spanning tree commands do not function under Brocade VCS Fabric mode.

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

```
switch(conf-stp)# hello-time 5
```

See Also **forward-delay**, **max-age**

hold-time

Sets the time that a previously down backup router, which also must have a higher priority than the current master, will wait before assuming mastership of the virtual router.

Synopsis **hold-time** *range*

Operands

range	A value, in seconds, from 1 to 3600 that specifies the time a formerly down backup router waits before assuming mastership of the virtual router.

Default 0

Command Modes Virtual-router-group configuration mode

Description Sets the time that a previously down backup router, which also must have a higher priority than the current master, will wait before assuming mastership of the virtual router. The hold-time must be set to a number greater than the default of zero for this command to take effect.

Usage Guidelines This command can be used for both VRRP and VRRP-E.

Examples To set the hold time to 60 seconds for backup routers in a specific virtual router:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-Ve-25)# vrrp-extended-group 1
switch(config-vrrp-extended-group-1)# hold-time 60
```

See Also vrrp-group

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. Refer to "Usage Guidelines" below.
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 On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Spanning tree commands do not function under Brocade VCS Fabric mode.

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 [fibrechannel** *rbridge-id/slot/port* **|fcoe** *rbridge-id/slot/port* **|**
fortygigabitethernet *rbridge-id/slot/port* **| gigabitethernet** *rbridge-id/slot/port* |
port-channel *number* | **tengigabitethernet** *rbridge-id/slot/port* | **vlan** *vlan_id*]

no interface [port-channel *number* | **vlan** *vlan_id* | **fcoe** *rbridge-id/slot/port*]

Operands

fibrechannel *rbridge-id/slot/port*
Specifies a valid Fibre Channel port interface (Brocade VDX 6730 switches only in Brocade VCS Fabric mode).

rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

fcoe *rbridge-id/slot/port*
Specifies a valid FCoE port interface.

rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

fortygigabitethernet	Specifies a valid 40 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
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.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface (Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches only).
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
vlan *vlan_id*	Specifies the VLAN number. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Global configuration mode

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

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

The **fibrechannel** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6730-32 and Brocade VDX 6730-76 switches in Brocade VCS Fabric mode. The prompt for configuring these ports is in the following format:

```
switch(config-FibreChannel-66/0/1)#
```

The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8. The prompt for configuring these ports is in the following format:

```
switch(config-if-gi-22/0/1)#
```

Examples To configure a Fibre Channel port on a Brocade VDX 6730-32 switch:

```
switch(config)# interface FibreChannel 66/0/1
switch(config-FibreChannel-66/0/1)#
```

To enter FCoE configuration mode for an interface:

```
switch(config)# interface fcoe 1/0/1
switch(config-Fcoe-1/3/10)#
```

To enter configuration mode on a 1 Gbps interface on a Brocade VDX 6710:

```
switch(config)# interface gigabitethernet 1/0/1
switch(config-if-gi-1/0/1)#
```

See Also interface management, interface vlan, interface Ve, show interface

interface loopback

Configures a loopback interface.

Synopsis **interface loopback** *port_number*

no interface loopback *port_number*

Operands

port_number	Specifies the port number for the loopback interface. The range is 1 to 255.

Defaults None.

Command Modes Rbridge subconfiguration mode (for VCS)

Global configuration mode (for standalone)

Description Use this command to configure a loopback interface. Loopback is a logical interface traditionally used for stable routing operation.

Usage Guidelines Use the **no interface loopback** *port_number* command to remove the loopback interface.

Example The following example shows the steps needed to create a loopback interface with a port number of 25. Also, an Rbridge ID of 11 is used in this example. This example is for a VCS environment.

```
switch(config)# rbridge-id 11
switch(config-rbridge-id-11)# interface loopback 25
```

See Also **interface**, **interface vlan**

interface management

Configures the management interface.

Synopsis **interface management** *rbridge-id/port*

ip address *ipv4_address/prefix_len* [**dhcp**]

no ip address *ipv4_address/prefix_len* [**dhcp**]

ip access-group *IP_ACL*

no ip access-group *IP_ACL*

ip gateway-address *ipv4_address*

no ip gateway-address *ipv4_address*

ipv6 address {*ipv6_address/prefix_len* [*dhcp* | **autoconfig**]}

no ipv6 address {*ipv6_address/prefix_len* [*dhcp* | **autoconfig**]}

ipv6 access-group *IP_ACL*

no ipv6 access-group *IP_ACL*

speed {**10** | **100** | **auto**}

no speed

Operands

rbridge-id/port Specifies the management interface to be configured as the *rbridge-id* followed by a slash (/) and the port number.

port On compact switches, the port number for the management port is always 0.

On a modular switches with two redundant management modules, can configure two management ports, 1 and 2.

ip address Configures the management IP address in IPv4 format.

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.

ip access-group Applies an access list to the IPv4 management interface.

IP_ACL **in** Specifies the access list (ACL) name to be applied to the ingress direction. You can apply up to 63 ACLs.

ip gateway-address Configures the management IP gateway address in IPv4 format.

ipv4_address
Specified the IP gateway address in IPv4 format.

ipv6 Configures the management IP address in IPv6 format using a prefix.

ipv6_address/prefix_len
Specified the IP address in IPv6 format using a prefix.

autoconfig Enables IPv6 stateless auto-configuration. This option is valid only on the interface rbridge-id/1, but it enables auto-configuration for the entire chassis.

dhcp Enables dynamic host configuration protocol (DHCP) on the management port.

ipv6 access-group
Applies an access list to the IPv6 management interface.

IP_ACL **in** Specifies the access list (ACL) name to be applied to the ingress direction. You can apply up to 63 ACLs.

speed Sets the speed for the management interface. Valid speed values are:

10 10 Mbps Full Duplex

100 100 Mbps Full Duplex

auto Auto negotiation (default)

Defaults DHCP is disabled by default.

IPv6 stateless auto-configuration is disabled by default.

The default speed setting is auto negotiation.

Command Modes Global configuration mode

Description Use this command to configure the management interface. This command supports IP addresses in IPv6 and IPv4 format. This command enters a management interface configuration mode where you can choose configuration parameters for IPv4 and IPv6 addresses.

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. For the other operands, use the **no** option to remove the corresponding configuration.

A static IPv6 address and stateless auto-configuration can co-exist.

Auto-configuration is configured chassis-wide and you configure it always under **interface management** *rbridge-id/1*. Once the feature is configured under **interface management** *rbridge-id/1* it is configured for both management interfaces.

Examples To configure a management interface with a static IPv4 IP address on a Brocade VDX 6730:

```
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-1/0)# speed 100
```

To apply an ACL to the management interfaces on the Brocade VDX 8770-4:

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ip access-group stdACL3 in
switch(config-Management-1/1)# ipv6 access-group stdV6ACL1 in
switch(config-Management-1/1)# exit
switch(config)# interface Management 1/2
switch(config-Management-1/2)# ip access-group extdACL5 in
switch(config-Management-1/2)# exit
```

To enable DHCP for IPv4 addresses:

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ip address dhcp
```

To enable DHCP for IPv6 addresses:

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ipv6 address dhcp
```

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

interface Ve

Configures a virtual ethernet interface.

Synopsis **interface ve** *vlan_id*

no interface ve *vlan_id*

Operands

vlan_id	Specifies the corresponding VLAN interface that must already be configured before the Ve interface can be created.

Defaults None.

Command Modes Rbridge subconfiguration mode (for VCS).

Global configuration mode (for standalone).

Description Use this command to configure a virtual ethernet interface. Before you can configure a Ve interface, you must configure a VLAN interface. The corresponding Ve interface must use the same VLAN ID you used to configure the VLAN.

Usage Guidelines Use the **no interface ve** *vlan_id* command to remove the Ve interface. This will not remove the corresponding VLAN interface.

Example The following example shows the steps needed to create a Ve interface with the VLAN ID of 56, assuming the VLAN 56 interface has already been created. Also, an Rbridge ID of 11 is used in this example. This example is for a VCS environment.

```
switch(config)# rbridge-id 11
switch(config-rbridge-id-11)# int ve 56
```

See Also **interface**; **interface vlan**

interface vlan

Configures VLAN.

Synopsis **interface vlan** *vlan_id*

no interface vlan *vlan_id*

Operands *vlan_id* Specifies the VLAN interface to configure.

Defaults VLAN 1 is predefined on the switch.

Command Modes Global configuration mode

Description Use this command to configure 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.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Use the **no interface vlan** *vlan_id* command to delete a VLAN interface. This would also delete a corresponding Ve interface.

Examples To create a VLAN with ID 56:

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

See Also **interface**, **interface Ve**, **fcmap**, **shutdown (STP)**, **switchport**

ip access-group

Applies rules specified in a MAC ACL to traffic entering an interface.

Synopsis **ip access-group** *name* [**in | out**]

no ip access-group *name* [**in | out**]

Operands

name	Specifies the name of the standard or extended IP access list.
in | out	Specifies the binding direction (ingress or egress).

Defaults There are no access lists applied to the interface.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te, Ve)

Description Use this command to apply a IP ACL to a Layer 2 or a VLAN interface. You create the IP ACL by using the **mac access-list** global configuration command.

Usage Guidelines You can assign one IP ACL (standard or extended) to an interface.

When a packet is received on an interface with a IP 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 specified ACL does not exist, the switch permits all the packets.

Use the **no ip access-group** *name* [**in | out**] command to remove the IP ACL from the interface.

Examples To apply an ingress IP ACL named *ipacl2* on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip access-group ipacl2 in
```

To remove an ingress IP ACL named *ipacl2* from a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no ip access-group ipacl2 in
```

See Also **interface**, **interface Ve**, **ip access-list**, **resequence**

ip access-list

Creates a standard or extended access control list (ACL) and, once created, configures a set of rules to define traffic parameters on the ACL.

Synopsis

[**ip** | **ipv6**] **access-list** [**standard** | **extended**] [*name*]

no [**ip** | **ipv6**] **access-list** [**standard** | **extended**] [*name*]

[**seq num** | **no seq num**] **access list** [**permit** | **deny**] [**any** | **host** *IP_addr*]

[**seq num** | **no seq num**] **access list** [**permit** | **deny**] [**tcp** | **udp**] [**any** | **host** *IP_addr*] [**any**] [**eq** *port*] [**range** *range_of_ports*] | [**gt** | **lt** | **neq** | **dscp** *value* | **ack** | **fin** | **rst** | **sync** | **urg** | **psh** | **log**]

no [**seq num**] *access list*

Operands

[seq num | no seq num] access list
Specifies the sequence number of the access list. The number must be from 0 through 65535 (applies to both standard and extended ACLs).

ip | **ipv6**
Specifies the IP type. An ACL can contain rules for only one version of IP (either IPv4 or IPv6).

standard | **extended**
Specifies one of the following types of IP Access-lists:

Standard
Contains rules for just only Source IP address. The rules are applicable to all the ports of that source IP address.

Extended
Contains rules for a combination of IP Protocol, Source IP, Destination IP, and Destination Port.

name
Specifies the name of the ACL. Each ACL has a unique name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hypen.

permit | **deny**
Specifies whether to permit or deny traffic for the combination specified in the rule. (applies to both standard and extended ACLs).

any | **host** *ip-addr*
Specifies the IP address of the host from which inbound traffic must be filtered (applies to both standard and extended ACLs).

any
The IP address of the host to which egress or control outbound traffic must be blocked. Since the egress and outbound traffic is blocked, the destination address is always “any” (which also covers the Virtual IP address of a host).

tcp | **udp**
Specifies the type of protocol used for management access.

eq
Specifies if there is only one destination port that must be filtered through the ACL rule.

port
Indicates the destination port for which the filter is applicable. This is applicable for both UDP and TCP. The port number range is from 0 through 65535.

range
Specifies a range of ports to filter through the ACL rule.

range_of_ports
Indicates the range of ports for which the filter is applicable.

gt	This policy applies to TCP or UDP port numbers greater than the port number, or are the numeric equivalent of the port name you enter after the gt parameter.
lt	This policy applies to TCP or UDP port numbers that are less than the port number, or are the numeric equivalent of the port name you enter after the lt parameter.
neq	The policy applies to all TCP or UDP port numbers, except the port number or port name you enter after the neq parameter.
dscp *value*	Compares the specified value against the DSCP value of the received packet. The range of valid values is from 0 through 63.
ack, **fin**, **rst**, **sync**, **urg**, **psh**	Any combination of the TCP flags may be specified.
log	Packets matching the filter is sent to the CPU and a corresponding log entry is generated. The optional log parameter enables the logging mechanism. This option is only available with permit and deny.

Defaults None

Command Modes Global configuration mode

Description Use this command to create an IP ACL and to apply a set of rules to the standard or extended ACL.

Usage Guidelines

- Each ACL must have a unique name.
- An ACL can contain rules for only one version of IP (either IPv4 or IPv6).
- Only one ACL for each version of IP (IPv4 or IPv6) can be applied to the Management interface. The factory default configuration of the switch consists of one IPv4 and one IPv6 address applied to the Management interface.
- A filter (rule) is identified by its unique sequence number and is only part of one ACL. Once the rules are defined, they cannot be re-defined.
- Us the **no** version of this command to delete a rule from the ACL.

Examples To create a standard ACL:

```
switch(config)# ip access-list standard stdACL3
switch(conf-ip-std)# exit
switch(config)# ip access-list extended extdACL5
switch(config-ip-ext)# exit
switch(config)# no ip access-list standard stdACL3
switch(config)# ipv6 access-list standard stdV6ACL1
switch(config-ipv6-standard)# exit
```

To create rules on a standard ACL:

```
switch(config)# ip access-list standard stdACL3
switch(config-ip-std)# seq 5 permit host 10.20.33.4
switch(config-ip-std)# seq 15 deny any
switch(config-ip-std)# exit
switch(config)# ip access-list standard stdACL3
switch(config-ip-std)# no seq 5
switch(config-ip-std)# exit
switch(config)# ipv6 access-list standard stdV6ACL1
switch(config-ipv6-std)# seq 10 permit
```

```
2001:db8:85a3:0:0:8a2e:370:7334
switch(config-ipv6-std)# seq 11 deny any
switch(config-ipv6-std)# exit
```

To create rules on an extended ACL:

```
switch(config)# ip access-list extended extdACL5
switch(config-ip-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
switch(config-ip-ext)# seq 7 deny tcp any any eq 80
switch(config-ip-ext)# seq 10 deny udp any any range 10 25
switch(config-ip-ext)# seq 15 permit tcp any any
switch(config-ip-ext)# exit
switch(config)# ip access-list extended extdACL5
switch(config-ip-ext)# no seq 7
switch(config-ip-ext)# no seq 5
switch(config-ip-ext)# exitswitch(config)#
switch#
```

See Also interface management, show running-config interface management, show running-config ip access-list

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 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 None

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Use this command to configure a primary or secondary IP address for a specific interface.

Usage Guidelines Use **no ip address** *ip-address/mask* [**secondary**] command to remove the IP address.

Multiple primary IP addresses are supported on an interface.

A primary IP address cannot overlap with a previously configured IP subnet.

A primary IP address must configured before you configure a secondary IP address in the same subnet.

Examples To configure a primary IP address on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip address 1.1.1.1/24
```

To configure a secondary IP address on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# ip address 1.1.1.1/28 secondary
```

See Also **interface**, **interface Ve**

ip arp-aging-timeout

Sets how long an ARP entry stays in cache.

Synopsis **ip arp-aging-timeout** *value*

no ip arp-aging-timeout

Operands

value	Determines how long an ARP entry stays in cache. The range is 0 to 240 (in minutes) for the gigabitethernet, tengigabitethernet, and fortygigabitethernet interfaces, and 0 to 35790 (in seconds) for Ve.

Defaults **IP arp-aging-timeout** is enabled by default and is set to 10 minutes.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve).

Description Use this command to configure how long an ARP entry stays in cache before the cache refreshes.

When the Brocade device places an entry in the ARP cache, the Brocade device also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

The ARP age affects dynamic (learned) entries only, not static entries.

Usage Guidelines Use the **no ip arp-aging-timeout** command to disable aging so that entries do not age out. The command **ip arp-aging-timeout** *0* also disables aging.

Examples To set the IP ARP aging timeout value to 100 minutes for a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip arp-aging-timeout 100
```

To disable IP ARP aging for a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no ip arp-aging-timeout
```

See Also **interface**, **interface Ve**

ip directed-broadcast

Enables IP directed broadcasts on an interface.

Synopsis **ip directed-broadcast**

no ip directed-broadcast

Operands None.

Defaults **IP directed broadcast** is disabled by default.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Use this command to enable IP directed broadcasts for a specific interface. A directed broadcast is an IP broadcast to all devices within a single directly attached network or subnet.

Usage Guidelines Use the **no ip directed-broadcast** command to disable IP directed broadcasts on a specific interface.

Examples To enable IP directed broadcasts on a specific **tengigabitethernet interface**:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip directed-broadcast
```

To disable IP directed broadcasts on a specific **fortygigabitethernet interface**:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no ip directed-broadcast
```

See Also **interface**, **interface Ve**

ip dns

Sets the domain name service (DNS) parameters.

Synopsis **ip dns {domain-name** *domain_name* |**name-server** *ip_address_of_name_server*}

no ip dns {domain-name *domain_name* |**name-server** *ip_address_of_name_server*}

Operands **domain-name** *domain_name*
The domain name for the primary and secondary name servers.

name-server *ip_address_of_name_server*
The IPv4 address of the primary and secondary name servers. IPv6 addresses are not supported

Defaults None.

Command Modes Global configuration mode

Description Use this command to configure the DNS domain name and name-server IP address. The DNS parameters are the domain name and the name server IP address for primary and secondary name servers

Usage Guidelines You can enter only two name server IP addresses and only IPv4 is supported.

Name servers can only be entered or removed one at a time. The newly-entered name server will append to the existing name server.

Examples **To configure DNS:**

```
switch(config)# ip dns domain-name  brocade.com
switch(config)# ip dns name-server  10.70.20.1
switch(config)# ip dns name-server  10.70.20.10
```

See Also **show running-config ip dns**

ip igmp last-member-query-interval

Sets the last member query interval.

Synopsis **ip igmp last-member-query-interval** *milliseconds*

no ip igmp last-member-query-interval

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 VLAN interface subconfiguration mode

Description Use this command to set the last-member query interval on a specific interface. The last-member query interval is the time in seconds that the IGMP router waits to receive a response to a group-specific query message, including messages sent in response to a host-leave message.

Usage Guidelines Use the **no ip igmp last-member-query-interval** command to reset to the default value.

Examples To set the last-member query interval to 1500 milliseconds on a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# ip igmp last-member-query-interval 1500
```

See Also **interface**, **ip igmp query-interval**, **ip igmp query-max-response-time**, **ip igmp static-group**

ip igmp query-interval

Sets the query interval.

Synopsis **ip igmp query-interval** *seconds*

no ip igmp query-interval

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 VLAN interface subconfiguration mode

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

Usage Guidelines Use the **no ip igmp query-interval** command to reset to the default value.

Examples To set the query interval to 500 seconds on a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# ip igmp query-interval 500
```

To remove the query interval **from a specific VLAN interface:**

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# no ip igmp query-interval
```

See Also **interface**, **ip igmp last-member-query-interval**, **ip igmp query-max-response-time**, **ip igmp static-group**

ip igmp query-max-response-time

Sets the maximum response time for IGMP queries.

Synopsis **ip igmp query-max-response-time** *seconds*

no ip igmp query-max-response-time

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 VLAN interface subconfiguration mode

Description Use this command to set the maximum response time for IGMP queries for a specific interface. When a host receives the query packet, it starts counting to a random value, less than the maximum response time. When this timer expires, the switch(host) replies with a report, provided that no other host from the same group has responded yet.

Usage Guidelines Use the **no ip igmp query-max-response-time** command to reset to the default value.

Examples To set the maximum response time to 20 seconds on a specific **VLAN interface**:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# ip igmp query-max-response-time 20
```

To remove the maximum response time from a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# no ip igmp query-max-response-time
```

See Also **interface**, **ip igmp last-member-query-interval**, **ip igmp query-interval**, **ip igmp static-group**

ip igmp snooping enable (global version)

Enables 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 enables IGMP snooping at the global level causing feature to be automatically enabled at all the already configured VLANs. In presence of this command, later if a VLAN is created, IGMP snooping will get enabled for that VLAN as well.

Examples To enable IGMP globally:

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

See Also **ip igmp snooping enable, show ip igmp snooping**

ip igmp snooping enable

Enables 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 is enabled on all VLAN interfaces.

Command Modes VLAN interface subconfiguration mode

Description Use this command to enable or disable IGMP snooping on a specific VLAN interface. IGMP snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Usage Guidelines Use the **no ip igmp snooping enable** command to disable snooping for a specific VLAN interface.

Examples To enable IGMP for a specific VLAN interface:

```
switch(config)# interface Vlan 1
switch(config-Vlan-1)# ip igmp snooping enable
```

To disable IGMP for a specific VLAN interface:

```
switch(config)# interface Vlan 1
switch(config-Vlan-1)# no ip igmp snooping enable
```

See Also **interface**, **ip igmp snooping enable (global version)**, **show ip igmp snooping**, **ip igmp snooping fast-leave**, **ip igmp snooping mrouter**, **ip igmp snooping mrouter-timeout**, **ip igmp snooping querier enable**

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 function is disabled by default.

Command Modes VLAN interface subconfiguration mode

Description Internet Group Management Protocol (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 To enable snooping fast-leave for a specific VLAN interface:

```
switch(config)# interface Vlan 1
switch(config-Vlan-1)# ip igmp snooping fast-leave
```

To disable snooping fast-leave for a specific VLAN interface:

```
switch(config)# interface Vlan 1
switch(config-Vlan-1)# no ip igmp snooping fast-leave
```

See Also **interface**, **ip igmp snooping enable (global version)**, **show ip igmp snooping**, **ip igmp snooping enable**, **ip igmp snooping mrouter**, **ip igmp snooping mrouter-timeout**, **ip igmp snooping querier enable**

ip igmp snooping mrouter

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

Synopsis **ip igmp snooping mrouter interface** {**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*}

no ip igmp snooping mrouter {**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*}

Operands

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

fortygigabitethernet
Specifies a valid 40 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet
Specifies a valid 10 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet Specifies a valid 1 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

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 Brocade VCS Fabric mode.

Defaults None

Command Modes VLAN interface subconfiguration mode

Description Use this command to configure a VLAN port member to be a multicast router interface, which is an interface that faces toward a multicast router or other Internet Group Management Protocol (IGMP) querier.

Usage Guidelines Use the **no ip igmp snooping mrouter** version of this command to remove the configured mrouter.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp snooping mrouter interface tengigabitethernet
101/0/1
```

See Also interface, ip igmp snooping enable (global version), show ip igmp snooping, ip igmp snooping enable, ip igmp snooping fast-leave, ip igmp snooping mrouter-timeout, ip igmp snooping querier enable

ip igmp snooping mrouter-timeout

Configures the mrouter timeout value for Internet Group Management Protocol (IGMP) snooping.

Synopsis **ip igmp snooping mrouter-timeout** *seconds*

no ip igmp snooping mrouter-timeout

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

Defaults Default value is 300 seconds.

Command Modes VLAN interface subconfiguration mode

Description This command sets the timeout range for when multicast router ports are automatically learned on a specific VLAN interface.

Usage Guidelines Use the **no ip igmp snooping mrouter-timeout** command to set the mrouter value to the default of 300 seconds on a specific VLAN interface.

Examples To configure the mrouter timeout value to 600 seconds on a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp snooping mrouter-timeout 600
```

See Also **interface**, **ip igmp snooping enable (global version)**, **show ip igmp snooping**, **ip igmp snooping enable**, **ip igmp snooping fast-leave**, **ip igmp snooping mrouter**, **ip igmp snooping querier enable**

ip igmp snooping querier enable

Activates or deactivates the Internet Group Management Protocol (IGMP) snooping querier.

Synopsis **ip igmp snooping querier enable**

no ip igmp snooping querier enable

Operands **None**

Defaults IGMP snooping querier is disabled by default.

Command Modes VLAN interface subconfiguration mode

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

Usage Guidelines Use **no ip igmp snooping querier enable** to disable IGMP snooping querier for a specific VLAN.

Examples To enable the IGMP snooping querier feature for a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp snooping querier enable
```

See Also **interface**, **ip igmp snooping enable (global version)**, **show ip igmp snooping**, **ip igmp snooping enable**, **ip igmp snooping fast-leave**, **ip igmp snooping mrouter**, **ip igmp snooping mrouter-timeout**

ip igmp static-group

Configures the static group membership entries for a specific interface.

Synopsis **ip igmp static-group** *A.B.C.D* **interface** {**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*}

no ip igmp static-group *A.B.C.D*

Operands

A.B.C.D Specifies the group address, as a subnet number in dotted decimal format (for example, 225.1.1.1), as the allowable range of addresses included in the multicast group.

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

fortygigabitethernet
Specifies a valid 40 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet
Specifies a valid 10 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet Specifies a valid 1 Gbps Ethernet interface.

rbridge-id Specifies the ID of the routing bridge. This is not valid in standalone mode.

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 64 for standalone mode. The range of valid values is from 1 through 6144 for Brocade VCS Fabric mode.

Defaults None

Command Modes VLAN interface subconfiguration mode

Description You can create IGMP static group membership to test multicast forwarding without a receiver host. When you enable IGMP static group membership, data is forwarded to an interface without receiving membership reports from host members. Using **ip igmp static-group**, packets to the group are fast-switched out of a specific interface. Static group membership entries are automatically added to the IGMP cache and mroute table.

Usage Guidelines Use the **no ip igmp static-group** version of this command to remove the configured static group.

Examples To create a static port-channel group for a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp static-group 10.0.0.1 interface port-channel 60
```

To reset a static group on a specific VLAN interface to the default settings:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# no ip igmp static-group 10.0.0.1
```

See Also interface, ip igmp last-member-query-interval, ip igmp query-interval, ip igmp query-max-response-time

ip load-sharing

Enables load sharing.

Synopsis **ip load-sharing** *paths*

no ip-load-sharing *paths*

Operands

paths	Specifies the number of load-sharing paths. The default is 8. The range is 0 to 8. If you specify 1, load sharing is disabled.

Default Load sharing is enabled and set to eight paths by default.

Command Modes Rbridge subconfiguration mode

Description Enables load sharing and sets the maximum number of load-sharing paths. By default, IP load sharing allows IP traffic to be balanced across up to eight equal paths. For optimal results, set the maximum number of paths to a value equal to or greater than the maximum number of equal-cost paths that your network typically contains. For example, if the Brocade device has six next-hop routers, set the maximum paths value to six.

Usage Guidelines Use the **no** parameter to remove the load sharing configuration and revert to its default value.

Examples To set the number of load-sharing paths to 7:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip load-sharing 7
```

ip mtu

Sets the MTU.

Synopsis **ip mtu** *size*

no ip mtu

Operands

size	Specifies the size of the maximum transmission unit (MTU) of an interface. The allowed MTU size is from 576 to 9018 bytes.

Defaults Default MTU size is 1500 bytes.

Command Modes Interface subconfiguration mode (fo, gi, te)

Description Use this command to specify the MTU on a specific interface.

Usage Guidelines The entire fabric acts like a single switch. Therefore, MTU is applicable only on edge-ports and not on an ISL.

Use the **no ip mtu** command to reset the MTU size to the default.

Examples To set the MTU size to 2000 bytes on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip mtu 2000
```

See Also interface

ip ospf area

Enables OSPF on an interface.

Synopsis **ip ospf area** *area-id*

no ip ospf area

Operands *area-id* Area address in dotted decimal or decimal format.

Default OSPF is disabled by default.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Enables an OSPF area on the interface to which you are connected.

Usage Guidelines Use the **no ip ospf area** command to disable OSPF on this interface.

Examples To enable a configured OSPF area named *0* on a specific OSPF tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf area 0
```

To enable a configured OSPF area named 0 on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 12
switch(config-Ve-12)# ip ospf area 0
```

See Also **interface**, **interface Ve**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf auth-change-wait-time

Configures authentication-change hold time.

Synopsis **ip ospf auth-change-wait-time** *wait-time*

no ip ospf auth-change-wait-time

Operands

wait-time	Time (in seconds) before an authentication change takes place. The range is 0 to 14400.

Default Default wait time is 300 seconds

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Sets/resets the authentication change hold time for the interface to which you are connected.

OSPF provides graceful authentication change for the following types of authentication changes:

- Changing authentication methods from one of the following to another of the following:
  - Simple text password
  - MD5 authentication
  - No authentication
- Configuring a new simple text password or MD5 authentication key.
- Changing an existing simple text password or MD5 authentication key.

Usage Guidelines Use the **no ip ospf auth-change-wait-time** command to reset the wait time to the default of 300 seconds.

Examples To set the wait time to 600 seconds on a specific OSPF tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/49
Switch(conf-if-te-190/0/49)# ip ospf auth-change-wait-time 600
```

To set the wait time to 400 seconds on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 12
switch(config-Ve-12)# ip ospf auth-change-wait-time 400
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf authentication-key

Configures simple password-based authentication for OSPF.

Synopsis **ip ospf authentication-key** {0 *password*| 2 *password* | 255 *password* | *password*}

no ip ospf authentication-key

Operands

0 *password*	No encryption. OSPF processes *password* as a plain text password and shows the unencrypted password in the **show running** command output as follows: `key 0 passwd`
2 *password*	Expects the user to provide the encrypted password, preceded by a *$* sign, and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`
255 *password*	Expects the user to provide the encrypted password, and *255* internally maps to *2*. OSPF shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`
password	OSPF processes *password* as a plain text password. OSPF internally encrypts this password as if encryption key 2 was specified and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

Default No authentication.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Sets or resets simple password-based authentication on the OSPF interface to which you are connected.

Usage Guidelines Use the **no ip ospf authentication-key** to disable OSPF authentication.

Examples The following command sets authentication only on the OSPF tengigabitethernet interface 190/0/49. To enter a plain text password called *brocade* that OSPF will encrypt as if encryption key 2 was specified:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf authentication-key brocade
```

The following command sets authentication only on the OSPF Ve interface 12. To enter a plain text password called *brocade* that OSPF will encrypt as if encryption key 2 was specified:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 12
switch(config-Ve-12)# ip ospf authentication-key brocade
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf cost

Configures cost for a specific interface.

Synopsis **ip ospf cost** *value*

no ip ospf cost

Operands *value* Cost value. Range is 1 to 65535.

Default Default cost value is 1.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Sets/resets the OSPF cost on the interface. If the cost is not configured with this command, OSPF calculates the value from the reference and interface bandwidths. For more information, see the **auto-cost reference-bandwidth** command.

Usage Guidelines Use the **no ip ospf cost** command to disable this configuration.

Examples To set the cost to 600 on a specific OSPF tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf cost 600
```

To set the cost to 520 on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 12
switch(config-Ve-12)# ip ospf cost 520
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**, **auto-cost reference-bandwidth**

ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

Synopsis **ip ospf database-filter** {**all-external** {**allow-default-and-type-4** | **allow-default-out** | **out**} | **all-out** | **all-summary-external** {**allow-default-and-type-4** | **allow-default-out** | **out**} }

Operands

all-external Blocks all external LSAs.

allow-default-and-type-4
Allows default-route LSAs and type 4 LSAs, but block all other LSAs.

allow-default-out Allows default-route LSAs, but block all other LSAs.

out

all-out Blocks all LSAs.

all-summary-external Blocks all summary (type 3) and external (type 5) LSAs.

no ip ospf database-filter all-external

no ip ospf database-filter all-out

no ip ospf database-filter all-summary-external

Default All filters are disabled.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description By default, the device floods all outbound LSAs on all the OSPF interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of the interfaces attached to the area.When enabled, this command blocks the specified outgoing LSAs on the interface. Some cases where you might want to enable filters are:

- To control the information being advertised to the network.
- To use a passive router for debugging only.

NOTE
You cannot block LSAs on virtual links.

Usage Guidelines Use the applicable completion of the **no ip ospf database-filter** command to disable this configuration.

Examples To apply a filter to block flooding of all LSAs on a specific OSPF fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# ip ospf database-filter all-out
```

To apply a filter to block flooding of all LSAs on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf database-filter all-out
```

See Also interface, interface Ve, ip ospf area, ip ospf auth-change-wait-time, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf md5-authentication, ip ospf mtu-ignore, ip ospf network, ip ospf passive, ip ospf priority, ip ospf retransmit-interval, ip ospf transmit-delay

ip ospf dead-interval

Configures neighbor dead interval.

Synopsis **ip ospf dead-interval** *interval*

no ip ospf dead-interval

Operands *interval* Dead interval in seconds.

Default 40

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Indicates the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down. If you change the dead interval, the hello interval is changed to be one fourth the new dead interval, unless the hello interval is also explicitly configured by using the **ip ospf hello-interval** command. Also, **running-config** displays only explicitly configured values of the hello interval, which means that a value that got automatically changed as the result of a dead-interval change would not be displayed.

Usage Guidelines Use the **no ip ospf dead-interval** command to use the default value.

Examples To set the dead interval to 80 on a specific OSPF fortygigabitethernet interface:

```
Switch(config)# interface fortygigabitethernet 101/0/10
Switch(conf-if-fo-101/0/10)# ip ospf dead-interval 80
```

To set the dead interval to 70 on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf dead-interval 70
```

See Also **interface**,**interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf hello-interval

Configures hello interval.

Synopsis **ip ospf hello-interval** *interval*

no ospf hello-interval

Operands *interval* Hello interval in seconds.

Default 10

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Configures the length of time between the transmission of hello packets that this interface sends to neighbor routers. If you change the hello interval, the dead interval is changed to be four times the new hello interval, unless the dead interval is also explicitly configured using the **ip ospf dead-interval** command. Also, **running-config** displays only explicitly configured values of the dead interval, which means that a value that got automatically changed as the result of a hello-interval change would not be displayed.

Usage Guidelines Use the **no ospf hello-interval** command to use the default value.

Examples To set the hello interval to 200 on a specific OSPF fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# ip ospf hello-interval 200
```

To set the hello interval to 180 on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf hello-interval 180
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf md5-authentication

Configures MD5 password and authentication change hold time.

Synopsis **ip ospf md5-authentication** {**key-activation-wait-time** *wait-time* | **key-id** *id MD5_key* {**0** | **2** | **255**} *ospf_password*}

no ip ospf md5-authentication key-id

Operands **key-activation-wait-time**. Sets the time that OSPF waits before activating a new key.

wait-time	Time (in seconds) OSPF waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. The default value is 300. The range is 0 to 14400.
key-id	Sets MD5 key and OSPF password.
id MD5_key	The *num* is a number from 1 – 255 and identifies the MD5 key that is being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the *key* is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.
0 *password*	No encryption. OSPF processes *password* as a plain text password and shows the unencrypted password in the **show running** command output as follows: `key 0 passwd`
2 *password*	Expects the user to provide the encrypted password, preceded by a *$* sign, and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`
255 *password*	Expects the user to provide the encrypted password, and *255* internally maps to *2*. OSPF shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`
password	OSPF processes *password* as a plain text password. OSPF internally encrypts this password as if encryption key 2 was specified and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

Default No authentication.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Sets/resets MD5 password and/or authentication change hold time on the interface to which you are connected.

Usage Guidelines Use the **no ip ospf md5-authentication key-id** command to disable this configuration.

Examples The following command sets authentication only on the OSPF fortygigabitethernet interface 100/0/1. To enter an MD5 id/key of **255 key** and a plain text OSPF password called *brocade* that OSPF will encrypt as if encryption key **2** was specified:

```
switch(config)# interface fortygigabitethernet 100/0/1
switch(conf-if-fo-100/0/1)# ip ospf md5 key-id 255 key brocade
```

The following command sets authentication only on the OSPF Ve interface 24. To enter an MD5 id/key of **255 key** and a plain text OSPF password called *brocade* that OSPF will encrypt as if encryption key **2** was specified:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf md5 key-id 255 key brocade
```

See Also **interface**,**interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf mtu-ignore

Enables or disables MTU-match checking.

Synopsis **ip ospf mtu-ignore**

no ip ospf mtu-ignore

Operands This command has no operands.

Default Enabled

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description In default operation, the IP MTU on both sides of an OSPF link must be the same, and a check of the MTU is performed when Hello packets are first exchanged. However, you can disable this check using the **no** parameter of this command.

Usage Guidelines Use the **no ip ospf mtu-ignore** command to disable MTU-match checking on a specific interface.

Examples To disable MTU-match checking on a specific OSPF fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# no ip ospf mtu-ignore
```

To disable MTU-match checking on a specific OSPF Ve interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# no ip ospf mtu-ignore
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf network

Configures network type.

Synopsis **ip ospf network** {**broadcast** | **point-to-point**}

Operands

broadcast	Network type is broadcast, such as ethernet.
point-to-point	Network type is point-to-point.

no ip ospf network

Default None.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Sets the network type for the interface.

Point-to-point can support unnumbered links, which requires less processing by OSPF.

Usage Guidelines Use the **no ip ospf network** command to remove the network-type configuration.

NOTE
The network type *non-broadcast* is not supported at this time.

Examples To configure an OSPF point-to-point link on the OSPF tengigabitethernet interface whose rbridge-ID/slot/port format is 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf network point-to-point
```

To configure an OSPF broadcast link on the OSPF Ve interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf network broadcast
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf passive**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf passive

Configures an interface as passive.

Synopsis **ip ospf passive**

no ip ospf passive

Operands This command has no operands.

Default All OSPF interfaces are active by default.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Sets the interface whose configuration mode you have entered to the passive state. Passive interfaces accept and process all OSPF protocol traffic, but they do not send any traffic. You might want to set an interface to passive mode if:

- You are planning to use the router mostly for debugging purposes.
- The router is a stub and does not route traffic.

Usage Guidelines Use the **no ip ospf passive** command to set an interface back to active.

Examples To set a specific OSPF tengigabitethernet interface to passive state:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf passive
```

To set a specific OSPF Ve interface to passive state:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf passive
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf priority**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf priority

Configures priority for designated-router (DR) election.

Synopsis **ip ospf priority** *value*

no ip ospf priority

Operands *value* Priority value. Range is 0 to 255.

Default 1

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Configures priority for DR election and backup-router election on the interface to which you are connected. The OSPF router assigned the highest priority becomes the designated router, and the OSPF router with the second-highest priority becomes the backup router.

Usage Guidelines Use the **no ip ospf priority** command to use the default value.

Examples To set a priority of 10 to the OSPF router that is connected to an OSPF tengigabitethernet interface 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf priority 10
```

To set a priority of 10 to the OSPF router that is connected to an OSPF Ve interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf priority 10
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf retransmit-interval**, **ip ospf transmit-delay**

ip ospf retransmit-interval

Configures retransmit interval.

Synopsis **ip ospf retransmit-interval** *rtx-int*

no ip ospf retransmit-interval

Operands *rtx-int* Retransmit interval in seconds. Range is 0 to 3600.

Default 5 seconds.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Configures the time between link-state advertisement (LSA) retransmissions to adjacent routers for this interface.

Usage Guidelines Use the **no ip ospf retransmit-interval** command to reset the retransmit interval to its default.

Examples To set the retransmit interval to 10 for all OSPF routers on the OSPF tengigabitethernet interface 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf retransmit 10
```

To set the retransmit interval to 50 for all OSPF routers on the OSPF Ve interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf retransmit 50
```

See Also **interface**, **interface Ve**, **ip ospf area**, **ip ospf auth-change-wait-time**, **ip ospf authentication-key**, **ip ospf cost**, **ip ospf database-filter**, **ip ospf dead-interval**, **ip ospf hello-interval**, **ip ospf md5-authentication**, **ip ospf mtu-ignore**, **ip ospf network**, **ip ospf passive**, **ip ospf priority**, **ip ospf transmit-delay**

ip ospf transmit-delay

Configures transmit delay for link-update packets.

Synopsis **ip ospf transmit-delay** *tx-delay*

no ip ospf transmit-delay

Operands *tx-delay* Transmit delay in seconds. Range is 0 to 3600.

Default 1 second.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Configures the estimated time required for OSPF to send link-state update packets on the interface to which you are connected.

Usage Guidelines Use the **no ip ospf transmit-delay** command to use the default value.

Examples To set a transmit delay of 10 seconds for routers on the OSPF tengigabitethernet interface 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf transmit-delay 10
```

To set a transmit delay of 30 seconds for routers on the OSPF Ve interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface Ve 24
switch(config-Ve-24)# ip ospf transmit-delay 30
```

See Also interface, interface Ve, ip ospf area, ip ospf auth-change-wait-time, ip ospf authentication-key, ip ospf cost, ip ospf database-filter, ip ospf dead-interval, ip ospf hello-interval, ip ospf md5-authentication, ip ospf mtu-ignore, ip ospf network, ip ospf passive, ip ospf priority, ip ospf retransmit-interval

ip prefix-list

Configures the ip prefix-list instance.

Synopsis **ip prefix-list** *name instance* [**permit** | **deny**] *A.B.C.D/MLEN* **ge** *value* **le** *value*

no ip prefix-list *name instance* [**permit** | **deny**] *A.B.C.D/MLEN* **ge** *value* **le** *value*

Operands *name*

instance

permit

deny

A.B.C.D/MLEN

ge *value*

le *value*

Defaults None

Command Modes Privileged EXEC mode

Description This command configures the ip prefix-list instance.

Usage Guidelines Use the **no ip prefix-list** command to disable this feature.

Examples None

See Also **match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set ip next-hop, set metric, set tag**

ip proxy-arp

Enables proxy ARP on an interface.

Synopsis **ip proxy-arp**

no ip proxy-arp

Operands None

Defaults Proxy ARP is enabled by default.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve)

Description Use this command to enable proxy ARP on a specific interface. Proxy ARP allows the Brocade device to answer ARP requests from devices on one network on behalf of devices in another network. Because ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Therefore, ARP requests do not cross routers.

Usage Guidelines Use the **no ip proxy-arp** command to disable proxy ARP on a specific interface.

Examples To enable proxy ARP on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip proxy-arp
```

To disable proxy ARP on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no ip proxy-arp
```

See Also **interface**, **interface Ve**

ip route

Adds a static route.

Synopsis **ip route** *A.B.C.D/L A.B.C.D* [*metric*] [**distance** *distance*] [**tag** *tag*]

ip route *A.B.C.D/L* {**fortygigabitethernet** *rbridge-id/slot/port*| **gigabitethernet** *rbridge-id/slot/port*| **port-channel** *number*| **tengigabitethernet** *rbridge-id/slot/port*| **ve** *vlan#*} [*metric*] [**distance** *distance*] [**tag** *tag*]

ip route *A.B.C.D/L* **null** *rbridge-id/slot/port* [*metric*] [**distance** *distance*] [**tag** *tag*]

no ip route *A.B.C.D/L A.B.C.D*

no ip route *A.B.C.D/L* {**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **tengigabitethernet** *rbridge-id/slot/port* | **ve** *vlan#*}

no ip route *A.B.C.D/L* **null** *rbridge-id/slot/port*

Operands

A.B.C.D/L Specifies the destination IP address.

A.B.C.D Specifies the IP address of the next hop.

FortyGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 40-Gbps port outgoing interface.

rbridge-id Specifies the ID of the routing bridge.

slot Specifies a valid slot number.

port Specifies a valid port number.

GigabitEthernet *rbridge-id/slot/port*
Specifies a valid 1-Gbps Ethernet outgoing interface

rbridge-id Specifies the ID of the routing bridge.

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 1 through 6144.

TenGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 10-Gbps Ethernet outgoing interface.

rbridge-id Specifies the ID of the routing bridge.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan#* Specifies the vlan number.

null *rbridge-id/slot/port* Drops packets with this destination.

rbridge-id Specifies the ID of the routing bridge.

slot Specifies a valid slot number.

port Specifies a valid port number.

metric	Cost metric of the route. Default is 1. Range is 1 to 16.
distance *distance*	Specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, the Brocade device prefers lower administrative distances over higher ones. Default is 1. Range is 1 to 255.
tag *tag*	Tag value of the route to use for route filtering with a route map. Range is 0 to 4294967295.

Default See default values listed within the descriptions of the operands.

Command Modes Rbridge subconfiguration mode

Description Adds a static route to IP routing tables.

Usage Guidelines You can use the **no** parameter to remove a static route.

Examples To configure a static route to 10.95.7.0, using 10.95.6.157 as the next-hop gateway.

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route 10.95.7.0/24 10.95.6.157
```

ip route next-hop ospf

Enables static-route next-hop-resolution with OSPF routes.

Synopsis **ip route next-hop ospf**

no ip route next-hop ospf

Operands There are no operands for this command.

Default Disabled

Command Modes Rbridge subconfiguration mode

Description Enables the Brocade device to use routes learned from a specified protocol to resolve a configured static route.

Usage Guidelines You can use the **no** parameter to disable static-route next-hop-resolution with OSPF routes.

Examples To enable static-route next-hop-resolution with OSPF routes:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route next-hop ospf
```

ip route next-hop-enable-default

Enables the default route for next-hop resolution.

Synopsis **ip route next-hop-enable-default**

no ip route next-hop-enable-default

Operands There are no operands for this command.

Default Disabled

Command Modes Rbridge subconfiguration mode

Description Enables the Brocade device to use the default route (0.0.0.0/0) to resolve a next hop.

This command works independently from the **ip route next-hop-recursion** and **ip route next-hop ospf** commands. If the default route is a protocol route, that protocol needs to be enabled to resolve static routes using the **ip route next-hop ospf** command. If the default route itself is a static route, you must configure the **ip route next-hop-recursion** command to resolve other static routes by this default route.

Usage Guidelines Use the **no** parameter to disable the default route for next-hop resolution.

Examples To enable the default route for next-hop resolution:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route next-hop-enable-default
```

ip route next-hop-recursion

Enables the Brocade device to use routes to resolve another route.

Synopsis **ip route next-hop-recursion** *level*

no ip route next-hop-recursion

Operands

level	Sets the number of levels of recursion allowed. Default is 3. Range is 0 to 10.

Default Next-hop recursion level is 3 by default.

Command Modes Rbridge subconfiguration mode

Description Enables next-hop recursive lookup by other routes, and set the next-hop recursion level. If you want to disable the recursion configuration, set the value to 0. You can re-enable the configuration later.

Usage Guidelines Use the **no ip route next-hop-recursion** command to remove next-hop resolution configuration and revert to its default.

Examples To set the next-hop recursion level to 7:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route next-hop-recursion 7
```

ip router-id

Configures router ID.

Synopsis **ip router-id** *A.B.C.D*

no ip router-id *A.B.C.D*

Operands

A.B.C.D	Specifies the IPv4 address that you want as the router ID.

Default None

Command Modes Rbridge subconfiguration mode

Description Configures a router ID, which is a 32-bit number that uniquely identifies the device. By default, the router ID is the numerically lowest IP interface configured on the device. If you prefer, you can explicitly set the router ID to any valid IP address. The IP address should not be in use on another device in the network.

Usage Guidelines Use the **no ip router-id** *A.B.C.D* command to remove the router ID and use the default router ID.

Examples To specify a router ID of 192.158.1.2:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip router-id 192.158.1.2
```

ipv6 route

Configures the preferred route for the management interface.

Synopsis **ipv6 route** *value*

no ipv6 route *value*

Operands **route** *value* Sets the route for the management interface.

Defaults None

Command Modes Global configuration mode

Description This command configures the preferred route for the management interface.

Usage Guidelines The **no** option of this command removes the configuration.

Examples How to set the IPv6 route for the management interface.

```
switch(config)# ipv6 route fe80::21b:edff:fe0b:3c00/64
```

See Also **interface management**

iscsi-priority

Sets the iSCSI priority bitmap.

Synopsis **iscsi-priority** *value*

no iscsi-priority

Operands

value	The priority bitmap value. The valid range of values is from 0 through 7.

Defaults The default value is 4.

Command Modes Protocol LLDP configuration mode

Description This command allows the user to set the iSCSI priority bitmap for use in the DCBX iSCSI TLV. Use the **no iscsi-priority** command to return to the default value.

Usage Guidelines None

Examples None

See Also None

isl-r_rdy

Sets the flow control primitive used to prevent frame drop to ISL R_RDY mode.

Synopsis **isl-r_rdy**

no isl-r_rdy

Operands None

Defaults The default value is **no isl-r_rdy**, or VC_RDY flow control mode.

Command Modes Interface Fibre Channel configuration submode

Description Use this command to enable interswitch link receiver ready (ISL R_RDY) flow control mode on a Fibre Channel port.

This flow control mode can be enabled only for a port configured for long distance operation with long distance modes LE, LD, or LS.

In ISL R_RDY mode, the port sends the R_RDY primitive signal that the port is ready to receive frames. The port sends an exchange link parameter (ELP) with flow control mode 02. If a port is ISL R_RDY enabled, it can only receive an ELP with flow control mode 02. A received ELP with flow control mode 01 will segment the fabric.

Use the **no** version of this command to disable ISL R_RDY mode on a port, and instead establish VC_RDY flow control.

Usage Guidelines We recommend disabling ISL R_RDY.

This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

A Fibre Channel port configured as a trunk port cannot have the ISL R_RDY flow control enabled.

Examples To enable ISL R_RDY mode on a port:

```
switch(config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# isl-r_rdy
```

To disable ISL R_RDY mode on a port:

```
switch(config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# no isl-r_rdy
```

See Also **desire-distance, fill-word, interface, long-distance, show running-config interface FibreChannel, shutdown, speed (Fibre Channel), trunk-enable, vc-link-init**

keep-alive timeout (fabric-map)

Enables or disables the keep-alive timeout.

Synopsis **keep-alive timeout**

no keep-alive timeout

Operands None

Defaults None

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 **fabric-map, fcoe**

l2traceroute

The **l2traceroute** 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 **l2traceroute**

Operands See Usage Guidelines.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

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 **l2traceroute** command allow for generating frames with similar properties as the ones generated from a connected device, thus traversing the same path through the fabric.

Usage Guidelines This command does not support operands. You are prompted for the required information after you enter the **l2traceroute** command.

Configuration results depend on the configuration options you select. The following fields display when you enter the **l2traceroute** command:

- **Source MAC address**—Enter the source MAC address. The MAC address must be a valid MAC address that exists in the mac-address-table.
- **Destination MAC address**—Enter the destination MAC address. The MAC address must be a valid MAC address that exists in the mac-address-table.
- **Vlan**—Enter the VLAN number. On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.
- **Edge rbridge-id**—Enter the edge Rbridge ID on which the **l2traceroute** command is to run.
- **Extended commands**—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.

Based on the input for Extended commands, if you enter **Y**, the options branch as follows:

- **Protocol Type** [IP]—Enter the protocol type. You must select IP.
  - Source IP address—Enter the source IP address.
  - Destination IP address—Enter the destination IP address.
- **IP Protocol Type** [TCP |UDP|0-255]—Enter the IP protocol type.
  - 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.
  - 0-255 is the numeric protocol value. to use as filter.

- Source port number—Enter the source port number. The valid port range is from 0 through 65535. This is an optional field.
- Dest port number—Enter the destination port number. The valid port range is from 0 through 65535. This is an optional field.

Examples Example of extended commands, IP protocol type, and TCP as the IP protocol type.

```
switch# l2traceroute
Source mac address                 : 0050.564f.549f
Destination mac address            : 0005.1ea0.8dd8
Vlan [1-3583]                      : 1
Edge rbridge-id [1-239]            : 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/0-255]   : TCP
Source port number [0-65535]       : 58
Dest port number [0-65535]         : 67

switch# l2traceroute
Source mac address                 : 0000.0000.1111
Destination mac address            : 0000.0000.2222
Vlan [1-3583]                      : 1
Edge rbridge-id [1-239]            : 50
Extended commands [Y/N]?           : n
Rbridge    Ingress                    Egress                     Rtt(usec)
--------------------------------------------------------------------------------
50         Te 50/0/15                 Te 50/0/38(isl)            0
40         Te 40/0/38(isl)            Te 40/0/2(isl)             60322
10         Te 10/0/2(isl)             Te 10/0/4(isl)             1274
20         Te 20/0/4(isl)             Te 20/0/10(isl)            1119
30         Te 30/0/10(isl)            Te 30/0/19                 1787
```

See Also None

lacp port-priority

Sets port priority for an interface.

Synopsis **lacp port-priority** *value*

no lacp port-priority

Operands

value	Specifies the priority. The range is 1 to 65535. A lower number takes priority over a higher number.

Defaults The default LACP port priority value is 32768.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description Use this command to set the priority of the physical interface for LACP.

An LACP port priority is configured on each port using LACP. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

A link with higher priority (smaller in value) gets preference over a link with lower priority (greater in value).

Usage Guidelines Use the **no lacp port-priority** command to return to the default value.

Example To set the LACP port priority to 1000 for a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lacp port-priority 1000
```

See Also interface

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
```

See Also None

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 that a long-timeout value of 30 seconds will be used. With this value, the port waits three times this long (90 seconds) before invalidating the information received earlier on this PDU.
short	Specifies that a short-timeout value of one second will be used. With this value, the port waits three times this long (three seconds) before invalidating the information received earlier on this PDU.

Defaults For Brocade trunks, the default value is the **short** timeout, and for standard LAGs, the default value is the **long** timeout.

Command Modes Interface subconfiguration mode (fo, gi, te)

Description Use this command to set the timeout value based on how frequently you think the switch will receive LACP PDUs from the partner switch.

Usage Guidelines Use the **no lacp timeout** command to return to the default operand.

Examples To use the LACP long-timeout value on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lacp timeout long
```

See Also **interface**

ldap-server host

Configures an LDAP-server host.

Synopsis **ldap-server host** {*ipaddr* | *FQDN*} [**port** *portnum*] [**basedn** *basedn*] [**timeout** *secs*] [**retries** *num*]

no ldap-server host {*ipaddr* | *FQDN*}

Operands

host {*ipaddr* | *FQDN*}
Specifies the IPv4 address or Fully Qualified Domain name of the Active Directory (AD) server. IPv6 is supported for Windows 2008 AD server only. The maximum supported length for the LDAP host name is 40 characters.

port *portnum*
Specifies theTCP port used to connect the AD server for authentication. The port range is 1024 to 65535.

domain *basedn*
Describes the base domain name of the host.

timeout *secs*
Specifies the wait time for a server to respond. The range is 1 to 60 seconds.

retries *num*
Specifies the number of retries for the server connection. The range is 0 to 100.

Defaults The default timeout is five seconds. The default port is 389. The default number of retries is five.

Command Modes Global configuration mode

Description Use this command to sets up a connection to the Lightweight Directory Access Protocol (LDAP) server host, or modifies an existing configuration.

Usage Guidelines The **no ldap-server host command** deletes the server configuration.

Use the **no** version of this command with an attribute to restore the default value.

Examples To add an LDAP server on port 3890 with retries set to three:

```
switch(config)# ldap-server host 10.24.65.6 basedn sec.brocade.com port 3890
retries 3
```

To change the domain in an existing configuration:

```
switch(config)# ldap-server host 10.24.65.6
switch(config-host-10.24.65.6)# domain security.brocade.com
```

To delete an LDAP server:

```
switch(config)# no ldap-server host 10.24.65.6
```

To reset the number of retries to the default value:

```
switch(config)# ldap-server host 10.24.65.6 retries
```

See Also **certutil import ldapca, ldap-server maprole, show running-config ldap-server**

ldap-server maprole

Maps an Active Directory (AD) group to a switch role.

Synopsis **ldap-server maprole group** *group_name* **role** *role_name*

no ldap-server maprole group *group_name*

Operands

group *group_name*	The name of the AD group.
role *role_name*	The name of the switch role.

Defaults None

Command Modes Global configuration mode

Description Use this command to map an Active Directory (AD) group to a switch role.

Usage Guidelines Use the no version of this command without the role operand to remove the mapping of the AD group to a role.

Examples To map the AD group “Administrator” to the switch role “admin”:

```
switch(config)# ldap-server maprole group Administrator role admin
```

To remove the mapping:

```
switch(config)# no ldap-server maprole group Administrator
```

See Also certutil import ldapca, ldap-server host, show running-config ldap-server

license add

Adds a license key to a switch.

Synopsis **license add licstr** *licenseString* [**rbridge-id** *ID*]

Operands

licstr *licenseString*	Specifies the license string to be added to the switch. The license string must be enclosed in double quotation marks. There is a maximum of 256 characters.
rbridge-id *ID*	Executes the command on the remote switch specified by the RBridge 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 ports for this command to take effect. Follow the instructions in the command output.

If you install a license on an unsupported platform, the operation succeeds, but the **license show** output indicates that the license is not supported.

In the Network OS v3.0.0 release this command is supported only on the local RBridge.

Examples To add a license on the local switch:

```
switch# license add licstr "*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#"

Adding license [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

To add a Dynamic Ports on Demand (DPOD) license on a switch that does not support the feature:

```
switch# license add licstr "*B
a6q3zwcUaNkWHPOfVf8afFZqHYype6sQxaEr5HIeFD3nba74i43BnRt6T8b2sDPtVMKuMfUPwV8NvHDX
xFgbB3f2w3pJNlujxLVdIVkXdoNHf6i4SzwuvimIj0ORN:JOojLU#"

License Added [*B
a6q3zwcUaNkWHPOfVf8afFZqHYype6sQxaEr5HIeFD3nba74i43BnRt6T8b2sDPtVMKuMfUPwV8NvHDX
xFgbB3f2w3pJNlujxLVdIVkXdoNHf6i4SzwuvimIj0ORN:JOojLU#]

switch# show license
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    Ports on Demand license - not applicable on this platform license
    Feature name:PORTS_ON_DEMAND_1
```

See Also **license remove, show license, show license id**

license remove

Removes a license key from a switch.

Synopsis **license remove licstr** {*licenseString* | *feature*} [**rbridge-id** *ID*]

Operands

licstr *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. Supported licensed features include the following: FCOE_BASE, PORTS_ON_DEMAND_1, PORTS_ON_DEMAND_2, VCS_FABRIC, ADVANCED_SERVICES, and LAYER_3.
rbridge-id *ID*	Executes the command on the remote switch specified by the RBridge 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 displayed in the **show license** command output to remove the license.

Depending on the feature being removed you must clear all license-related configurations, reboot the switch, or disable and re-enable the chassis or selected ports for this command to take effect. Follow the instructions in the command output.

This command deactivates but does not permanently remove time-based trial licenses.

You must disable or remove all configurations related to a licensed feature before you can remove the license for that feature.

In the Network OS v3.0.0 release this command is supported only on the local RBridge.

Examples To remove a license string from the local switch:

```
switch# license remove licstr "*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#

Removing license for rbridge-id 2 [*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

To remove a license based on the feature name from the local switch:

```
switch# license remove licstr "FCOE_BASE"
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.

The **line vty exec time-out** command is a configuration command and the timeout value set by this command holds for subsequent login sessions, unless it is overwritten for a single session with the **terminal timeout** command. The terminal timeout command is not a configuration command and the timeout value set by this command controls only the current session. After the current session times out, the **vty exec time-out** value applies for subsequent sessions.

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

This command is not available on the standby management module.

Examples To set the terminal timeout to 60 minutes:

```
switch(config)# line vty exec-timeout 60
switch(config-line-vty)# exit
switch(config)# exit
switch# show running-config line vty
line vty
exec-timeout 60
!
```

See Also **terminal**

linecard

Configures an interface module (line card).

Synopsis **linecard** *slot_number linecard_type*

no linecard slot_number

Operands

slot_number		Specifies the slot number to be configured. Interface module slots are 1 through 4 on the Brocade VDX 8770-4 and 1 through 8 on the Brocade VDX 8770-8.
linecard_type		Specifies the type of interface module. Supported types include the following:
	LC12x40G	12-port 40 GbE interface module
	LC48x1G	48-port 1 GbE interface module
	LC48x10G	48-port 10 GbE interface module
	LC72x1G	72-port 1 GbE interface module (Not supported)

Defaults None

Command Modes Global Configuration mode

RBridge configuration mode

Description Use this command to configure the specified slot for an interface module of a given type. The **no linecard** command removes the slot configuration.

The command is executed in the context of the given RBridge. You must first enter the rbridge-id context for the specific interface module. Once you are in the rbridge-id context, you execute the **linecard** *slot_number linecard_type* command to configure the slot.

Usage Guidelines If you replace a given interface module with another one of a different type, you must remove the configuration and then reconfigure the slot.

The interface module must be powered off before you can remove the slot configuration.

The LC72x1G type displayed under “possible completion” is not supported.

Examples To configure a slot for an interface module on a switch in VCS mode and to verify the configuration:

```
switch# configure
Entering configuration mode terminal
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# linecard 1 ?
Possible completions:
  LC12x40G   12X40G linecard
  LC48x1G    48X1G linecard
  LC48x10G   48X10G linecard
  LC72x1G    72X1G linecard
switch(config-rbridge-id-1)# linecard 1 LC48x10G
Creating new linecard configuration was successful.
switch(config-rbridge-id-1)# do show running-config rbridge-id 1 linecard
rbridge-id 1
  linecard 1 LC48x10G
```

```
linecard 4 LC48x10G
```

See Also show running-config rbridge-id linecard

lldp dcbx-version

Specifies which version of the Data Center Bridging Exchange (DCBX) protocol to use.

Synopsis **lldp dcbx-version** {**auto** | **cee**}

no lldp dcbx-version

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.

Defaults The default is auto.

Command Modes Interface subconfiguration mode (fo, gi, te)

Description Use this command to specify which version of the DCBX protocol to use for a specific interface. Devices enabled for data center bridging can use the DCBX protocol to discover and exchange information about their administratively configured capabilities. DCBX eliminates the need to configure a large number of switches in the network.

Usage Guidelines Use the **no lldp dcbx-version** command to return to the default setting.

Examples To specify that the CEE version be used on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp dcbx-version cee
```

See Also **interface**, **lldp disable, lldp iscsi-priority, lldp profile**

lldp disable

Disables the Link Layer Discovery Protocol (LLDP).

Synopsis **lldp disable**

no lldp disable

Operands None

Defaults By default, LLDP is enabled at both the global and interface levels.

Command Modes Interface subconfiguration mode (fo, gi, te)

Description Use this command to disable LLDP on the interface.

Usage Guidelines Use the **no lldp disable** command to enable LLDP on a specific interface.

Examples To disable LLDP on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp disable
```

To enable LLDP on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no lldp disable
```

See Also **interface**, **lldp dcbx-version, lldp iscsi-priority, lldp profile**

lldp iscsi-priority

Configures the priority that will be advertised in the DCBX iSCSI TLV.

Synopsis **lldp iscsi-priority** *value*

no lldp iscsi-priority

Operands *value* Specifies the priority value. The range of valid values is from 0 through 7.

Defaults The default priority value is 4.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description The iSCSI priority setting is used to configure the priority that will be advertised in the DCBX iSCSI TLV for a specific interface.

Usage Guidelines Use the **no lldp iscsi-priority** command to return to the default setting.

Examples To set the iSCSI priority value to 5 on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp iscsi-priority 5
```

See Also **interface**, **lldp dcbx-version, lldp disable, lldp profile**

lldp profile

Applies a Link Layer Discovery Protocol (LLDP) profile to an interface.

Synopsis **lldp profile** *name*

no lldp profile

Operands

name	Specifies the profile name. The maximum number of characters allowed is 32.

Defaults If the parameters are not defined in the profile, the default values are used.

Command Modes Interface subconfiguration mode (fo, gi, te)

Description Use this command to apply a Link Layer Discovery Protocol (LLDP) profile to a specific 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.

Use the **no lldp profile** command to delete the profile from the interface.

Examples To apply an LLDP profile called *test* on an specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp profile test
```

See Also **interface**, **lldp dcbx-version, lldp disable, lldp iscsi-priority**

logging auditlog class

Sets the severity levels for the audit log class.

Synopsis **logging auditlog class** *class*

no logging auditlog class *class*

Operands

class *class*	Specifies the class name of the audit log. Valid classes are CONFIGURATION, FIRMWARE, and SECURITY

Defaults The CONFIGURATION, FIRMWARE, and SECURITY audit log classes are enabled by default.

Command Modes Global configuration mode

Description Use this command to set the class for the audit log. Use the **no logging auditlog class** *class* command to reset the class number to the default value (INFO).

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

This command is not supported on the standby management module.

Example To enable the configuration class

```
switch(config)# logging auditlog class CONFIGURATION
```

See Also **clear logging auditlog, clear logging raslog**

logging raslog console

Sets the severity levels for the RASlog console.

Synopsis **logging rbridge-id** *rbridge-id* **raslog console** *severity*

no logging rbridge-id *rbridge-id* **raslog console**

Operands

rbridge-id *rbridge-id*	Specifies the rbridge 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 rbridge-id** *rbridge-id* **raslog console** command to reset the severity to the default value (INFO).

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

This command is not supported on the standby management module.

Examples To set the RASlog severity levels on switch 2:

```
switch(config)# logging rbridgeid 2 raslog console WARNING
```

To reset the RASlog severity levels to the default value.

```
switch(config)# no logging rbridgeid 2 raslog console
```

See Also **clear logging raslog, logging raslog console, show running-config logging**

logging rbridge-id raslog console

Sets the severity levels for the RASlog console.

Synopsis **logging rbridge-id** *rbridgeID* **raslog console** *severity*

no logging rbridge-id *rbridgeID* **raslog console**

Operands

rbridge-id *rbridgeID*	Specifies the rbridge 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 rbridge-id** *rbridgeID* **raslog console** command to reset the severity to the default value (INFO).

Usage Guidelines None

Examples To set the RASlog severity levels on switch 2:

```
switch(config)# logging rbridgeid 2 raslog console WARNING
```

To reset the RASlog severity levels to the default value.

```
switch(config)# no logging rbridgeid 2 raslog console
```

See Also **clear logging raslog, logging raslog console, show running-config logging**

logging syslog-facility local

Configures the syslog facility.

Synopsis **logging syslog-facility local** *log_level*

Operands

local *log_level*	Specifies the syslog facility level. Valid log levels include the following: LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7

Defaults The default syslog level is LOG_LOCAL7.

Command Modes Global configuration mode

Description Use this command to configure a switch to forward all error log entries to the one or more specified servers. You can configure up to four servers. Use the **no logging syslog-server** command to remove the specified IP address.

Usage Guidelines When used without a log level parameter, this command displays the current value.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples To configure the syslog facility level:

```
switch(config)# logging syslog-facility local LOG_LOCAL5
```

See Also **logging syslog-server. show running-config logging syslog-server**

logging syslog-server

Configures a switch to forward system messages to specified servers.

Synopsis **logging syslog-server** *ip_address* [*secure* {**true** | **false**}] [**port** [*value*]]

no logging syslog-server *ip_address* [*secure* {**true** | **false**}] [**port** [*value*]]

Operands

ip_address Specifies the IP address of the syslog server in IPv4 or IPv6 format.

secure {**true** | **false**}
Configures a secure syslog server. A secure port number with default values are not shown in the Brocade Network OS database. If the secure option is set to false, you are not able to set the port number.

port *value* Configures the port for the syslog server. The default value is 514.

Defaults If the secure operand is set to true and the port number is not specified, the default port number 6514 is used.

The default value for the secure operand is **false**.

Command Modes Global configuration mode

Description Use this command to configure a switch to forward all error log entries to the one or more specified servers. You can configure up to four servers. Use the **no logging syslog-server** command to remove the specified IP address.

The **certutil import syslog-ca** command is required for secure syslog to be fully functional.

Usage Guidelines You can configure up to four syslog servers. You must execute the command for each server.

This command is not supported on the standby management module.

In a Brocade VCS Fabric, the syslog configuration is distributed to all switches in the fabric.

If the secure option is set to false, you are not able to set the port number.

Examples To configure a server to which system messages are sent:

```
switch(config)# logging syslog-server 192.168.163.233
```

To remove a configured syslog server:

```
switch(config)# no logging syslog-server 192.168.163.233
```

See Also **certutil import syslogca, logging syslog-facility local, show running-config logging syslog-facility, show running-config logging syslog-server**

long-distance

Configures a Fibre Channel port to support long distance.

Synopsis **long-distance** {**l0** | **le** | **ld** | **ls**}

Operands

l0	Configures the port as a regular port. 20 full-size frame buffers are reserved for data traffic, regardless of the operating speed of the port. The maximum supported link distance is up to 5 km at 2 Gbps, up to 2 km at 4 Gbps, and up to 1 km at 8 Gbps.
le	Configures an E_Port distance greater than 5 km and up to 10 km. 5, 10, 20, and 40 full-size frame buffers are reserved for data traffic at port speeds of 1 Gbps, 2 Gbps, 4 Gbps, and 8 Gbps, respectively.
ld	Specifies automatic long distance configuration. The buffer credits for the given E_Port are automatically configured based on the actual link distance. Up to 1,452 full-size frame buffers are reserved depending on the distance measured during E_Port initialization. If a value for the desired distance is specified (**desire-distance** command), it is used as the upper limit to the measured distance.
ls	Configures a static long distance link with a fixed buffer allocation greater than 10 km. Up to 1,452 full-size frame buffers are reserved for data traffic, depending on the specified desired distance (**desire-distance** command).

Defaults The default value is **l0**.

Command Modes Fibre Channel interface subconfiguration mode

Description Use this command to allocate frame buffer credits to a port or to configure a specified long distance link.

Long distance configuration allows native Fibre Channel ports to run WAN/LAN connections. It ensures that the full bandwidth of a link or trunk can be used for a particular long distance configuration. The receiving port must have sufficient buffers available, so that the transmitting port can fill the link with enough frames to fill the entire length of the link. As the distance between switches and the link speed increases, additional buffer-to-buffer credits are required to maintain maximum performance. If a port is configured as a long distance port, the remaining ports of that port group could be disabled, fail to initialize, or move to “buffer limited” mode due to a lack of frame buffer credits.

Usage Guidelines This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

A long distance link can also be configured to be part of a trunk group.

The LE, LD, or LS levels can be enabled with ISL R_RDY mode of flow control over the long distance link. While using ISL R_RDY mode flow control, an E_Port cannot form trunk groups of long distance links even if the trunking is enabled.

Examples To configure a Fibre Channel port to support long distance links:

```
switch(config)# interface FibreChannel 8/0/1
switch(config-FibreChannel-8/0/1)# fill-word arbff-arbff
switch(config-FibreChannel-8/0/1)# long-distance ls
switch(config-FibreChannel-8/0/1)# desire-distance 100
switch(config-FibreChannel-8/0/1)# vc-link-init arb
switch(config-FibreChannel-8/0/1)# do show running-config interface FibreChannel
8/0/1
interface FibreChannel 8/0/1
     fill-word arbff-arbff
     long-distance ls
     vc-link-init arbff
     desire-distance 100
     no isl-r_rdy-mode
     no shutdown
```

See Also desire-distance, fill-word, interface, isl-r_rdy, long-distance-isl, show running-config interface FibreChannel, shutdown, speed (Fibre Channel), trunk-enable, vc-link-init

long-distance-isl

Extends an ISL link up to 10 km.

Synopsis **long-distance-isl** {**2000** | **5000** | **10000**}

no long-distance-isl

Operands

2000	Specifies a 2 km distant link.
5000	Specifies a 5 km distant link.
10000	Specifies a 10 km distant link.

Defaults The default value is 200 meters.

Command Modes Interface subconfiguration mode (Fibre channel, te)

Description An ISL port with PFC supports up to 10Km distance on eAnvil-based platforms. Up to 10Km links are lossless. You can have eight 1Km links forming a brocade trunk. You can also have mixed length cables forming the ISL. For ECMP purposes, you can have eight 8-link ECMP trunks.

Usage Guidelines For a 10 Km ISL link, no other ISL links are allowed on the same ASIC.

For 2 Km and 5 Km ISL links, another short distance ISL link can be configured.

A maximum of three PFCs can be supported on a long distance ISL link.

Use the **no long-distance-isl** command to revert to the default value.

This command does not function on the Brocade VDX6720-24.

Examples To extend the support of an ISL port with PFC by a distance of 5 Km on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# long-distance-isl 5000
```

See Also **interface, isl-r_rdy, long-distance**

mac access-group

Applies rules specified in a MAC access control list (ACL) to traffic entering or exiting an interface.

Synopsis **mac access-group** *name* {**in** | **out**}

no mac access-group *name* {**in** | **out**}

Operands

name	Specifies the name of the standard or extended MAC access list.
in	Specifies to filter inbound packets only.
out	Specifies to filter outbound packets only.

Defaults There are no access lists applied to the interface.

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te, Vlan)

Description Use this command to apply a MAC ACL to a supported interface. You create the MAC ACL by using the **mac access-list** global configuration command.

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 specified ACL does not exist, the switch permits all the packets.

Use the **no mac access-group** {**in** | **out**} command to remove the MAC ACL from the interface.

Examples To apply an ingress MAC ACL named *macacl2*, and to filter inbound packets only, on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# mac access-group macacl2 in
```

To remove an ingress MAC ACL named macacl2 from a specific port-channel interface:

```
switch(config)# interface port-channel 62
switch(conf-Port-channel-62)# no mac access-group macacl2 in
```

See Also **interface, mac access-list extended**, **mac access-list standard**

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 63, and the name must start with a letter ‘a’ to ‘z’, ‘A’ to ‘Z’, or a number ‘1’ to ‘9’. No special characters are allowed except underscore and hypen.

Defaults None

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 **no 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(conf-macl-ext)# no mac access-list extended mac1
switch(config)#
```

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 extended access list. The maximum character limit is 63, and the name must start with a letter ‘a’ to ‘z’, ‘A’ to ‘Z’, or a number ‘1’ to ‘9’. No special characters are allowed except underscore and hypen.

Defaults None

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(conf-macl-std)# no mac access-list standard mac1
switch(config)#
```

See Also **deny (extended ACLs), deny (standard ACLs), permit (extended ACLs), permit (standard ACLs)**

mac-address-reduction

Enables or disables the MAC address reduction feature.

Synopsis **mac-address-reduction** [**enable** | **disable**]

Operands

enable	Enables the MAC address reduction feature.
disable	Disables the MAC address reduction feature.

Defaults None

Command Modes Protocol Spanning Tree mode

Description This command either enables or disables the MAC address reduction feature.

Usage Guidelines None

Examples None

See Also 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* | **gigabitethernet** *rbridge-id/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 Brocade VCS Fabric 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 1 through 63.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
vlan *vlan_id*	Specifies the VLAN number. Refer to "Usage Guidelines" below.

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 **vlan** 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.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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

mac-rebalance

Forces the rebalancing of EXM entries for the MAC tables.

Synopsis **mac-rebalance port-channel** *number* {**rbridge-id** *rbridge-id*}

Operands

port-channel *number*	Specifies the port-channel interface number. The range of valid values is from 1 through 6144 for Brocade VCS Fabric mode.
rbridge-id *rbridge-id*	Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description To achieve complete utilization of the entire vLAG member links, MAC entries learnt on vLAG need to be equally distributed among the vLAG member nodes. There are some scenarios, in which the EXM entries may not be balanced equally among the vLAG member nodes.

Currently, EXM entries are balanced among the member nodes during RBridge membership changes (add or delete). MACs learned on vLAG are not re-balanced when the link updates (such as during LAG member additions or deletions), to avoid traffic disruption. However, when there are many link updates, the EXM mapping can become unbalanced and eventually overload the link capacity leading to frame drops. The mac-rebalance command corrects this scenario.

Usage Guidelines Run this command on all remote (non-VLAG) nodes.

This command is applicable to remote RBridge nodes, such as non-VLAG member nodes. However there are not any restrictions on the usage of this command in VLAG member nodes.

In Fabric Cluster mode, RBridge-IDs other than the curernt node's ID are not allowed.

This command does not function in standalone mode.

Examples In this example, the mac-rebalance command on RBridge 1 rebalances the EXM entries on RBridge 1 (for the vLAG 10).

```
switch# mac-rebalance port-channel 10 rbridge-id 1
```

See Also None

map

Enables the map configuration mode.

Synopsis **map default**

Operands None

Defaults None

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**

match interface

Configures the interface match clause in a route-map instance.

Synopsis **match interface** [**port-channel** | **Ve** | **Te** | **Gi** | **Fo**] *interface*

no match interface

Operands

port-channel	
Ve	Specifies a Virtual Ethernet interface.
Te	Specifies a TenGigabitEthernet interface.
Gi	Specifies a GigabitEthernet interface.
Fo	Specifies a FortyGigabitEthernet interface.
interface	The name of the interface. The operand can be up to 63 ASCII characters in length.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to configure the interface match clause in a route-map instance.

Usage Guidelines Use the **no match interface** to disable the feature.

Examples None

See Also **ip prefix-list, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set ip next-hop, set metric, set tag**

match ip address

Configures an IP prefix match clause in a route-map instance.

Synopsis **match ip address prefix-list** *plist_name*

no match ip address prefix-list *plist_name*

Operands

prefix-list *plist_name*	The name of the prefix list. The operand can be up to 63 ASCII characters in length.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to configure an IP prefix match clause in a route-map instance.

Usage Guidelines Use the **no match ip address prefix-list** *plist_name* to disable the feature.

Examples None

See Also **ip prefix-list, match interface, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set ip next-hop, set metric, set tag**

match ip next-hop

Configuring the IP next-hop match clause in a route-map instance.

Synopsis **match ip next-hop prefix-list** *plist_name*

no match ip next-hop prefix-list *plist_name*

Operands

prefix-list *plist_name*	The name of the prefix list. The operand can be up to 63 ASCII characters in length.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to configure the IP next-hop match clause in a route-map instance.

Usage Guidelines Use the **no match ip next-hop prefix-list** *plist_name* to disable the feature.

Examples None

See Also **match ip address, match interface, match metric, match tag, match route-type, route-map, set metric, set ip next-hop, set tag, set distance, ip prefix-list**

match metric

Configures the route metric match clause in a route-map instance.

Synopsis **match metric** *value*

no match metric *value*

Operands

value	This is the string to match. It can be an ASCII string up to 63 characters in length.

Defaults None

Command Modes Privileged EXEC mode

Description This command creates a route-map with a metric match criterion.

Usage Guidelines Use the **no match metric** *value* to disable the feature.

Examples None

See Also **ip prefix-list, match interface, match ip address, match ip next-hop, match route-type, match tag, route-map, set distance, set ip next-hop, set metric, set tag**

match route-type

Configures the route type clause in a route-map instance.

Synopsis **match route-type** [**internal** | **external-type1** | **external-type2**]

no match route-type [**internal** | **external-type1** | **external-type2**]

Operands

internal	Specifies an internal clause.
external-type1	Specifies an external type 1 clause.
external-type2	Specifies an external type 2 clause.

Defaults None

Command Modes Privileged EXEC mode

Description This command configures the route type clause in a route-map instance.

Usage Guidelines Use the **no match route-type** command to disable this feature.

This command is applicable only for OSPF routes.

Examples None

See Also **ip prefix-list, match interface, match ip address, match ip next-hop, match metric**, **match tag, route-map, set distance, set ip next-hop, set metric, set tag**

match tag

Configures the route tag match clause in a route-map instance.

Synopsis **match tag** *value*

no match tag *value*

Operands

value	This is the string to match. It can be an ASCII string up to 63 characters in length.

Defaults None

Command Modes Privileged EXEC mode

Description Matches routes with a specified name, to be used as the route map is referenced.

The match command can be any from the list of match commands defined later.

Usage Guidelines Use the **no match tag** *value* command to disable this feature.

Examples None

See Also **ip prefix-list, match interface, match ip address, match ip next-hop, match metric**, **match route-type**, **route-map, set distance, set ip next-hop, set metric, set tag**

max-age

Sets the interval time in seconds between messages that the spanning tree receives from the interface.

Synopsis **max-age** *seconds* [*vlan 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 vlan_id	Specifies the VLAN ID. Refer to "Description" below.

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.

If the VLAN parameter is not provided, the seconds value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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)

Spanning tree commands are only valid in standalone mode.

Examples To configure the maximum-age to 10 seconds:

```
switch(conf-rstp)# max-age 10
```

See Also **forward-delay, hello-time**

max-enodes

Configures the maximum number of FCoE devices that can be logged into a switch.

Synopsis **max-enodes** *value*

Operands

value	The number of allowed devices. The range of valid values is from 256 through 1000.

Defaults The default value is 256.

Command Modes FCoE fabric-map configuration mode

Description This command is primarily for dynamically increasing or decreasing the number of FCOE ports available to service logins.

For example, if the value of the max-enodes is 256, the maximum allowed logins on the switch is 256.

Usage Guidelines If the current number of active logins on the switch is same as the current value of **max-enodes**, the value cannot be decreased. The command fails with an appropriate error message.

When you increases the value of **max-enodes** and then decrease it again, the last-created ports are the first ones to be considered for deletion. For example, if you increase **max-enodes** from 256 to 356, and then return to 256, the ports that are considered for deletion will be from 356 to 256. However, if there are active logins on some of the ports between 256 and 356, those ports are not considered for deletion.

Examples None

See Also None

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.

This command functions only in standalone mode.

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**

max-metric router-lsa all-lsas

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Synopsis **max-metric router-lsa all-lsas**

Operands There are no operands for this command.

Default None

Command Modes Router configuration mode

Description When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the becomes a *stub router*, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Usage Guidelines Use the **no** parameter to disable advertising the maximum metric value in different LSAs.

Examples

```
switch(conf-ospf-router)# max-metric router-lsa all-lsas
```

metric-type

Configures the default metric type for external routes.

Synopsis **metric-type** {**type1** | **type2**}

Operands

type1	The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.
type2	The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

Default **type1**

Command Modes Router configuration mode

Usage Guidelines Use the **no** parameter to return to the default setting.

Examples To set the default metric type for external routes to type2:

```
switch(conf-ospf-router)# metric-type type2
```

See Also **default-information-originate**

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 32.

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 To set the minimum number of links to 16 on a specific port-channel interface:

```
switch(config)# interface port-channel 33
switch(config-Port-channel-33)# minimum-links 16
```

See Also **minimum-links**

mode

Sets the LLDP mode on the switch.

Synopsis **mode** {**tx** | **rx**}

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.

Usage Guidelines None

Examples To enable only the transmit mode:

```
switch(conf-lldp)#mode tx
```

To enable only the receive mode:

```
switch(conf-lldp)#mode rx
```

See Also **show lldp interface**

monitor session

Enables a Port Mirroring session for monitoring traffic.

Synopsis **monitor session** *session_number*

no monitor session *session_number*

Operands

session_number	Specifies a session identification number. The range of valid values is from 0 through 23.

Defaults None

Command Modes Global configuration mode

Description Use this command to enable a session for monitoring traffic. Use the **no monitor version of this** command to delete the port mirroring 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 22 for monitoring traffic:

```
switch(config)#monitor session 22
switch(config-session-22)#source tengigabitethernet 0/1 destination
tengigabitethernet 0/15 direction both
```

See Also source

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 2 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 None

Examples To set the number of consecutive misses:

```
switch(conf-lldp)#multiplier 2
```

See Also **hello**

neighbor

Manually configures a neighbor.

Synopsis **neighbor** *A.B.C.D*

Operands *A.B.C.D* **IPv4 address of the neighbor.**

Default Neighbors are not configured by default.

Command Modes Router configuration mode.

Description Configures a neighbor and is typically used in point-to-point networks. OSPF Hellos must use a unicast address, not broadcast or multicast packets.

Usage Guidelines Use the **no** parameter to remove the neighbor.

Examples To configure a neighbor whose IPv4 address is 1.1.1.1:

```
Switch(conf-ospf-router)# neighbor 1.1.1.1
```

no certutil ldapca

Deletes CA certificates

Synopsis **no certutil ldapca**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command deletes the CA certificates of all Active Directory servers.

Usage Guidelines None

Examples None

See Also **certutil import ldapca**, **ldap-server host**,**ldap-server maprole**, **show running-config ldap-server**

nssa-translator

Configures Not So Stubby Area (NSSA) Type 7-to-Type 5 Link State Advertisement (LSA) translation.

Synopsis nssa-translator

Operands This command has no operands.

Default Translation is enabled.

Command Modes Router configuration mode.

Description Enables or disables NSSA Type 7-to-Type 5 LSA translation on the NSSA Area Border Router (ABR). Translation may be needed if routers within the NSSA need to know about external routes. However, disabling this translation can be useful when the router is an area border router with many NSSA areas, and does not need to export the NSSA external routes into the backbone.

Usage Guidelines Use the **no** parameter to disable NSSA Type 7-to-Type 5 translation.

Examples To disable NSAA Type 7-to-Type 5 LSA translation:

```
Switch(conf-ospf-router)# no nssa-translator
```

ntp server

Specifies or adds an NTP server IP address.

Synopsis **ntp server** *ip-address*

no ntp server *ip-address*

Operands

ip-address	Specifies the NTP server IPv4 IP address (dot-decimal notation) or the IPv6 IP address (hexadecimal colon-separated notation).

Defaults The NTP server list is LOCL (no NTP server configured).

Command Modes Global configuration mode

Description Use this command to add an NTP server IPv4 or IPv6 address to a list of server IP addresses,

Usage Guidelines The maximum number of NTP servers allowed is 5. The **no** operand removes an NTP server IP address. Removing the current active NTP server resets the ntp status to “LOCL” until a new, active server is selected.

Network Time Protocol (NTP) commands must be configured on each individual switch.

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 ntp status, show clock**

oscmd

Provides a command shell for selected Linux commands.

Synopsis **oscmd** *Linux command*

Operands

Linux command	The following Linux commands are supported with **oscmd**:
arp [**-a**]	Displays the Address Resolution Protocol (ARP) tables.
cat	Concatenates files and displays to standard output.
cp	Copies files and directories in a file system.
ftp	Transfers files to and from a remote server.
ifconfig [*netmask*] [**up**]	Configures the active network interface.
ls [**-al**] [*path*]	Lists files and directories on the switch.
mkdir *dir*	Creates a directory.
mv [**i**] *file1 file2*	Renames a file or directory.
rm [-**rf**] *file*	Removes a file or directory.
rmdir	Removes a directory.
tcpdump	Analyzes network traffic. The following options are supported with the Network OS implementation. Refer to the Linux documentation for more information on how to use this command.

- **-AbdDefIKlLnNOpqRStuUvxX**
- **-B** *buffer_size*
- **-c** *count*
- **-C** *file_size*
- **-G** *rotate_seconds*
- **-F** *file*
- **-i** *interface*
- **-m** *module*
- **-M** *secret*
- **-r** *file*
- **-s** *snaplen*
- **-T** *type*
- **-w** *file*
- **-W** *filecount*
- **-E** *spi@ipaddr*
- **-y** *datalinktype*
- **-z** *postrotate-command*
- **-Z** *user* [*expression*]

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to execute selected Linux commands on the switch.

Usage Guidelines Refer to the Linux man pages for more information on the supported commands.

The **oscmd** command is disabled under FIPS mode.

Examples To display the ARP table:

```
switch# oscmd arp -a
? (127.2.1.9) at ac:de:48:02:09:07 [ether] on eth2
? (127.2.1.7) at ac:de:48:02:07:07 [ether] on eth2
? (10.17.16.3) at 00:1b:ed:0b:90:00 [ether] on eth0
? (10.17.16.1) at 02:e0:52:5a:36:5c [ether] on eth0
? (10.17.19.14) at 00:14:22:20:5c:3c [ether] on eth0
? (127.2.2.9) at ac:de:48:02:09:08 [ether] on eth2
```

To copy a file to a remote server:

```
switch# oscmd rcp file root@127.2.1.8:
switch#
switch:FID128:root> telnet 127.2.1.8
Trying 127.2.1.8...
Connected to 127.2.1.8.
Escape character is '^]'.

Linux 2.6.34.6 (sw0) (0)

sw0 login: root
Password:
sw0:L2/0: >ls
.profile  .rhosts  file
```

To copy a file using secure copy:

```
switch# oscmd scp file file1 hegdes@10.31.2.27:
hegdes@10.31.2.27's password:  file
100%    0     0.0KB/s   00:00 file1
100%    0     0.0KB/s   00:00
```

See Also None

password-attributes

Configures switch-wide user password attributes.

Synopsis **password-attributes** [**min-length** *minlen*] [**max-retry** *maxretry*] [**character-restriction** [**upper** *numupper*] [**lower** *numlower*]] [**numeric** *numdigits*] [**special-char** *numsplchars*]]

no password-attributes [**min-length** *minlen*] [**max-retry** *maxretry*] [**character-restriction**]

Operands

min-length *minlen*	Specifies the minimum length of the password. Set the minimum from 8 through 32 characters. The default is 8 characters.
max-retry *retry*	Specifies the number of failed password logins permitted before a user is locked out. The lockout threshold can range from 0 through 16. The default value is 0.
character-restriction	Configures the restriction on various types of characters.
upper *numupper*	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 *numlower*	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 *num*	Specifies the minimum number of numeric characters that must occur in the password. The number of numeric characters can range from 0 through 32 characters. The default is 0.
special-char *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.

Defaults Refer to the operand section.

Command Modes Global configuration mode

Description Use this command to configure global password attributes.

Usage Guidelines The **no** form of the **password-attributes** command sets the specified password attributes to the default values.

Examples To configure global password attributes and to verify the configuration:

```
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
```

To reset the character restriction attributes and to verify the configuration:

```
switch(config)# no password-attributes character-restriction lower
switch(config)# no password-attributes character-restriction upper
switch(config)# exit

switch# show running-config password-attributes
password-attributes max-retry 4
password-attributes character-restriction numeric 0
password-attributes character-restriction special-char 0
```

To clear the global password attributes:

```
switch(config)# no password-attributes
switch(config)# exit
switch# show running-config password-attributes
% No entries found.
```

See Also rule, service password-encryption, show running-config password-attributes

pdu-rx-limit

Sets the number of PDU packets received on an ELD-enabled port before detecting and breaking a loop.

Synopsis **pdu-rx-limit** *limit*

no pdu-rx-limit *limit*

Operands

limit	The number of PDU packets. The valid range is 1 through 5.

Defaults The default limit is 1.

Command Modes ELD configuration mode.

Description Use this command to determine how many PDU packets are to be received before a loop is assumed to exist and ELD disables a port to break the loop. This command sets the same value for every routing bridge in the Brocade VCS Fabric cluster. Use the **no pdu-rx-limit** command to reset the limit to its default value of 1.

Use this command with the **hello-interval** command to determine the time taken to detect a loop. The time taken to detect a loop is the product of the pdu-rx-limit and the hello interval. The Brocade VCS Fabric cluster in the loop with the lowest pdu-rx-limit is the cluster where the loop gets broken, assuming that the hello limit is correctly set to the same value on all routing bridges.

Usage Guidelines This command applies only in Brocade VCS Fabric mode.

This functionality detects Layer 2 loops only.

Example To set the limit on the number of PDU packets received to 4:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# pdu-rx-limit 4
```

See Also **edge-loop-detection VLAN, edge-loop-detection port-priority, hello-interval, protocol edge-loop-detection, show edge-loop-detection globals**

permit (extended ACLs)

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

Synopsis **permit** {[**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [*EtherType* | **arp** | **fcoe** | **ipv4**] [**count**]}

no permit {[**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [*EtherType* | **arp** | **fcoe** | **ipv4**]}

Operands

any	Specifies any source MAC address.
host *MAC_ADDRESS*	**Specifies the source host MAC address for which to set permit conditions. Use the format HHHH.HHHH.HHHH.**
MAC_ADDRESS	**Specifies the destination host MAC address for which to set permit conditions. Use the format HHHH.HHHH.HHHH.**
any	Specifies any destination MAC address.
host *MAC_ADDRESS*	**Specifies the source host address for which to set permit conditions. Use the format HHHH.HHHH.HHHH.**
MAC_ADDRESS	**Specifies the destination host address for which to set permit conditions. Use the format HHHH.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_ADDRESS* | *MAC_ADDRESS*] parameters is specific to the source MAC address. The second set of [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] 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_ADDRESS* | **any**} [**count**]

no permit {*MAC_ADDRESS* | **any**}

Operands

MAC_ADDRESS	Specifies the source host MAC address for which to set permit conditions. Use the format HHHH.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 None

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)**

ping

Verifies network connectivity between a source and a destination.

Synopsis **ping** *dest-IPv4_addr* [**ipv6** *dest-ipv6-addr*] [*host-name*] [**count** [*number]*] [**timeout** *seconds*] [**datagram-size** *bytes*] [**quiet**] [**numeric**]

Operands

dest-IPv4_addr	Specifies the IPv4 address of the destination device. This operand is valid only with the **ping** command.
ipv6 *dest-ipv6-addr*	Specifies the IPv6 address of the destination device. This operand is valid only with the **ping** command.
host-name	Destination host name.
count *number*	Specifies the number of transmissions (pings). The range is 1 through 655350; the default is 5.
timeout *seconds*	Specifies the number of seconds in between transmissions. The range is 1 through 60; the default is one second.
datagram-size *bytes*	Specifies the datagram-size (also known as the maximum transmission unit, or MTU) IN bytes. The range is 36 through 9100; the default is 56 bytes.
quiet	Prints only the first and last line of the command output.
numeric	Do not lookup hostnames.

Defaults Refer to the operand descriptions for specific defaults.

Command Modes Privileged EXEC mode

Description Use this command to probe IP connectivity to another computer or device on a TCP/IP network. This command sends a specified number of pings with configured parameters to the specified destination device.

Usage Guidelines None

Example To ping an IPv4 destination address:

```
switch# ping 172.16.4.80
Type Control-c to abort
PING 172.16.4.80 (172.16.4.80): 56 data bytes
64 bytes from 172.16.4.80: icmp_seq=0 ttl=120 time=101.466 ms
64 bytes from 172.16.4.80: icmp_seq=1 ttl=120 time=122.914 ms
64 bytes from 172.16.4.80: icmp_seq=2 ttl=120 time=145.637 ms
64 bytes from 172.16.4.80: icmp_seq=3 ttl=120 time=170.032 ms
64 bytes from 172.16.4.80: icmp_seq=4 ttl=120 time=103.036 ms
--- 172.16.4.80 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 101.466/128.617/170.032/26.188 ms
```

To ping an IPv4 destination address in quiet mode:

```
switch# ping 172.16.4.80 quiet
Type Control-c to abort
PING 172.16.4.80 (172.16.4.80): 56 data bytes
```

```
--- 172.16.4.80 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 100.605/146.372/192.552/32.505 ms
```

To ping an IPv6 destination address in numeric mode with a data-gram size.

```
switch# ping ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 count 3 datagram-size 48
numeric timeout 3
Type Control-c to abort
PING fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470):
48 data bytes
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=0 ttl=64
time=6.356 ms
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=1 ttl=64
time=0.170 ms
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=2 ttl=64
time=0.171 ms
--- fec0:60:69bc:92:218:8bff:fe40:1470 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.170/2.232/6.356/2.916 ms
```

See Also traceroute

police-priority-map

Creates color-based priority CoS mapping. A police-priority-map remaps frame CoS values to conform or exceed color values when rates conform or exceed limits set in a classification map.

Synopsis

police-priority-map *name*

no police-priority-map *name*

conform *CoS values*

exceed *CoS values*

Operands

name	Name of police-priority-map
CoS values	CoS priority values (0, 1, 2, 3, 4, 5, 6, 7)

Defaults

If you do not define priority mapping for a color (conform or exceed), the map defaults to priorities 0, 1, 2, 3, 4, 5, 6, and 7.

Command Modes

Global configuration mode

police-priority-map configuration (config-policemap) mode

Description

Use this command to configure a police-priority-map. When you launch the **police-priority-map** command, the system is placed in config-policepmap mode for the configured map. At this point, you can remap CoS values to conform or exceed color values.

Usage Guidelines

This command creates a police-priority-map. Use the **conform** *CoS values* or **exceed** *CoS values* commands while in config-policemap mode to remap 802.1p CoS values that are conforming to CIR values set in the policy-map or exceeding CIR values, but conforming to EIR values set in the policy-map. Use the **no police-priority-map** *name* command while in global configuration mode to remove the police-priority-map. Use the **no conform**|**exceed** *CoS values* command while in **config-policepmap** mode to remove CoS remapping.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples

To create a priority-map and place system into config-policepmap mode to configure conform and exceed color mapping:

```
switch(config)# police-priority-map pmap1
switch(config-policepmap)# conform 0 1 1 2 1 2 1 1
switch(config-policepmap)# exceed 3 3 3 3 4 5 6 7
```

To remove the conform class mapping while in config-policepmap mode:

```
switch(config-policepmap)# no conform
```

To remove the class-map while in global configuration mode:

```
switch(config)# no police-priority-map pmap1
```

See Also

show running-config police-priority-map

policy-map

Configures a policy-map containing a class-map so that you can apply Policer and QoS attributes to a particular interface.

Synopsis **policy-map** *policy-map name*

no policy-map *policy-map name*

Operands *policy-map name* Name of police policy-map

Defaults No created policy-map.

Command Modes global configuration mode

policy map configuration (config-policymap) mode

Description Use this command to configure a police policy-map. When you launch the **policy-map** command, the system is placed in config-policymap mode for the configured map. At this point, you can add a class-map containing policing parameters to the policy-map. Refer to "class" on page 52.

Usage Guidelines This command creates a Policer policy-map to apply Policer and QoS attributes to a particular interface. Each policy-map can contain one class-map. The class-map can be associated with specific policing and QoS parameters. Use the **no policy-map** *name* command while in global configuration mode to remove the policy-map. Associate the policy-map to the interface for inbound or outbound direction with the **service-policy** command.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To create a policy-map and place system into config-policymap mode so that you can add a class-map:

```
switch(config)# policy-map policymap1
switch(config-policymap)#
```

To remove the policy-map while in global configuration mode:

```
switch(config)# no policy-map policymap1
```

See Also **class, qos cos, show policymap, show running-config class-map, show running-config policy-map**

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 None

This command functions only in standalone mode.

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
```

See Also None

port-profile

Creates a new AMPP port-profile in the fabric.

Synopsis **port-profile** *profile-name* [**activate** | **qos-profile** | **security-profile** | **vlan-profile** | **static** *mac-address*]

no port-profile *profile-name*

Operands

profile-name	A fabric-wide unique name of a port-profile.
activate	Activates the specified profile
qos-profile	Enters directly into edit mode for the QoS sub-profile.
security-profile	Enters directly into edit mode for the security sub-profile.
vlan-profile	Enters directly into edit mode for the VLAN sub-profile.
static *mac-address*	Statically associates the profile VM MAC address.

Defaults None

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.

Security profiles are applied to the ACLs based on the profile or PolicyID. Therefore, multiple security profiles can be applied to the same profiled port.

Usage Guidelines Use the **no port-profile sample-profile activate** version of the command to de-activate the port-profile.

Examples None

See Also None

port-profile-port

Activates the Automatic Migration of Port Profiles (AMPP) port-profile configuration mode on a port.

Synopsis **port-profile-port**

no port-profile-port

Operands None

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to activate AMPP port-profile configuration mode on a specific port. AMPP management allows you to associate AMPP port profiles with VMware port groups, and provides a port profile comparison tool to easily compare port profiles within or across fabrics for robust VM migration.

Usage Guidelines Use the **no port-profile-port** command to remove the complete AMPP configuration from the selected port.

Examples To activate AMMP port-profile configuration mode on a specific tengigabitethernet-interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# port-profile-port
```

See Also **interface**

power-off linecard

Powers off an interface module (line card).

Synopsis **power-off linecard** *slot_number*

Operands

slot_number	Specifies the slot number to be powered-off. Interface module slots are 1 through 4 on the Brocade VDX 8770-4 and 1 through 8 on the Brocade VDX 8770-8.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to power-off an interface module. An interface module must be powered-off before you can change the slot configuration.

Usage Guidelines None

Examples To power off an interface module in slot 4:

```
switch# power-off linecard 4
```

See Also linecard, power-on linecard, show running-config rbridge-id linecard

power-on linecard

Powers on an interface module (line card).

Synopsis **power-on linecard** *slot_number*

Operands

slot_number	Specifies the slot number to be powered-on. Interface module slots are 1 through 4 on the Brocade VDX 8770-4 and 1 through 8 on the Brocade VDX 8770-8.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to power-on an interface module.

Usage Guidelines None

Examples To power off an interface module in slot 4:

```
switch# power-on linecard 4
```

See Also linecard, power-off linecard, show running-config rbridge-id linecard

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 None

Examples

```
switch(config-cee-map-default)# precedence 1
```

See Also None

preempt-mode

Turns on preempt mode for a virtual router session.

Synopsis **preempt-mode**

no preempt-mode

Operands None

Default Enabled for VRRP; Disabled for VRRP-E.

Command Modes Virtual-router-group configuration mode.

Description Configures preempt mode. When set, the highest-priority backup router will always be the master if the owner is not available. If not set, a higher priority backup will not preempt a lower-priority master.

Usage Guidelines This command is for VRRP and VRRP-E. You can use the **no** parameter with this command to turn off preempt mode. For VRRP-E, the interface must be **ve**.

Examples To turn on preempt mode for a virtual-router-group-1 session:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# preempt-mode
```

See Also **vrrp-group, vrrp-extended-group**

priority

Sets the priority of a physical router in a virtual router group.

Synopsis **priority** *range*

Operands

range	A value from 1 to 254 that sets the priority of a physical router in a virtual router group. Higher numbers have priority over lower numbers.

Default 100

Command Modes Virtual-router-group configuration mode.

Description Configures the priority of a physical router in a virtual router group. When set, the highest priority backup router will always be the master. (For VRRP, however, the owner is always the master if it is available.) If not set, a higher priority backup will not preempt a lower priority backup that is acting as master.

For an owner router in VRRP, the priority automatically becomes 255 if the virtual IP address of the virtual router and the real IP address of the owner are the same.

Usage Guidelines You can perform this command for VRRP or VRRP-E.

Examples To set the priority to 110 for the VRRP virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# priority 110
```

To set the priority to 110 for the VRRP-E virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int ve 25
switch(config-Ve-25)# vrrp-group-extended 1
switch(config-vrrp-extended-group-1)# priority 110
```

See Also vrrp-group, vrrp-extended-group

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

Description 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 2 Bandwidth allocation to user priority groups

PGID	PG%	PFC	Description
0	50	Y	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 To define the CEE map and configure the bandwidth with the priority group, use the values in Table 2.

```
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)**, **show qos maps**, **show running-config cee-map**

priority-tag

Toggles priority-tagging support.

Synopsis **priority-tag**

no priority-tag

Operands None

Defaults By default, the priority-tag is disabled for all supported interfaces.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description This command toggles the priority-tagging support on a specific interface. This command is the only method for toggling priority-tagging.

Usage Guidelines Use the **no priority-tag** command to disable priority-tagging support.

Example To enable priority-tagging support on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# priority-tag
```

See Also **interface, cee-map (FCoE)**

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 **lldp 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 **lldp profile**

prom-access disable

Disables access to the Boot PROM for FIPS compliance.

Synopsis **prom-access disable**

Operands None

Defaults By default, the Boot PROM is accessible.

Command Modes Privileged EXEC mode

Description Use this command to disable access to the boot PROM for compliance with FIPS.

In non-FIPS compliant mode, you can access the Boot PROM by holding down the ESC key during the 4-second period when the switch is booting up. In FIPS compliant state, PROM access is disabled to prevent users from net-installing firmware.

Usage Guidelines Under normal operating conditions, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "**fibranne**" to make the command available.

Use this command only when preparing a switch for FIPS compliance.

CAUTION

Once disabled, you cannot re-enable Boot PROM access.

Examples To disable access to the Boot PROM:

```
switch# unhide fips
Password: *****
switch# prom-access disable
You are disabling PROM access. Do you want to continue? [yes/no] (no): yes
switch# PROM access Disabled
```

See Also cipherset, fips root disable, fips selftests, fips zeroize, show prom-access, unhide fips

protect-mode enable

Enables protect mode.

Synopsis **protect-mode enable**

no protect-mode enable

Operands None

Defaults None

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

See Also None

protocol edge-loop-detection

Sets the edge-loop detection (EDL) configuration mode.

Synopsis **protocol edge-loop-detection**

Operands None

Defaults ELD configuration mode is not set.

Command Modes Global configuration mode.

Description Use this command to enter the ELD configuration mode to make changes to the ELD configuration.

Usage Guidelines This functionality detects Layer 2 loops only.

Examples To enter the ELD configuration mode:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)#
```

See Also **hello-interval, pdu-rx-limit, shutdown-time**

protocol lldp

Enters the Link Layer Discovery Protocol (LLDP) configuration mode.

Synopsis **protocol lldp**

no protocol lldp

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 the operands to the default settings.

Usage Guidelines None

Examples To reset all LLDP configurations:

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

See Also None

protocol spanning-tree

Designates the context for spanning tree.

Synopsis **protocol spanning-tree** {**mstp** | **rstp** | **stp** | **pvst** | **rpvst**}

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 Plus (PVST+).
rpvst	Specifies Rapid Per-VLAN Spanning Tree Protocol Plus (R-PVST+).

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.

This command does not function in VCS mode.

Brocade Network OS v3.0.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

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 None

Command Modes Functions in all modes except privileged EXEC 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 None

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)#
```

See Also None

qos cos

Specifies the interface Class of Service (CoS) value.

Synopsis **qos cos** *value*

no qos 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 subconfiguration mode (fo, gi, Port-channel, te).

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.

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.

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.

Use the **no qos cos** command to return the CoS value to the default.

Examples To set the CoS value to 2 on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# qos cos 2
```

To return the CoS value to the default on a specific port-channel interface:

```
switch(config)# interface port-channel 22
switch(config-Port-channel-22)# no qos cos
```

See Also **interface, qos map cos-traffic-class, qos trust cos, show qos interface**

qos cos-mutation

Applies a CoS-to-CoS mutation quality of Service (QoS) map on an interface.

Synopsis **qos cos-mutation** *name*

no qos 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 subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to apply a CoS-to-CoS mutation QoS map on a specific interface. Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Usage Guidelines 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 a CoS-to-CoS mutation QoS map named *test* on a specifc fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# qos cos-mutation test
```

To remove a CoS-to-CoS mutation QoS map from a specific port-channel interface:

```
switch(config)# interface port-channel 22
switch(config-Port-channel-22)# no qos cos-mutation
```

See Also **interface, 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 subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to apply a CoS-to-Traffic Class QoS map to a specific interface.

Usage Guidelines This command is not available when the interface is in the CEE Provisioning mode.

This command does not function in standalone mode.

Use the **no qos cos-traffic-class** command to remove the CoS-to-Traffic Class mapping.

Examples To apply a CoS-to-Traffic Class QoS map named *test* to a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos cos-traffic-class test
```

To remove CoS-to-Traffic Class QoS mapping from a specific port-channel interface:

```
switch(config)# interface port-channel 22
switch(config-Port-channel-22)# no qos cos-traffic-class
```

See Also **interface**, **qos cos-mutation**, **qos map cos-traffic-class**, **qos trust cos**, **show qos maps**

qos dscp-cos

Applies a defined DSCP-CoS map to an interface,

Synopsis **qos dscp-cos** *name*

no qos dscp-cos

Operands *name* Name of DSCP-to-COS mutation map

Defaults DSCP-to-CoS mutation is not enabled on interface.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to apply a DSCP-to-COS mutation map defined by the **qos map dscp-cos** *name* command to a specific interface.

Usage Guidelines The **qos dscp-cos** *name* command applies a defined DSCP-CoS mutation map to the interface. Use the **no qos dscp-cos** command while in the interface mode to remove the DSCP-CoS map from the interface.

Examples To apply a configured qos dscp-mutation map named *test* to a specific interface, enter the **qos dscp-cos** *name* command while in the interface subconfiguration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# qos dscp-cos test
```

To remove a configured qos dscp-mutation map named *test* from a specific interface, enter the **no qos dscp-cos** command while in the interface subconfiguration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# no qos dscp-cos
```

See Also **interface, qos dscp-mutation, qos map dscp-cos**, **show qos maps dscp-cos, qos dscp-cos**, **show qos maps dscp-cos**

qos dscp-mutation

Applies a defined DSCP mutation map to an interface,

Synopsis **qos dscp-mutation** *name*

no qos dscp-mutation

Operands *name* Name of DSCP mutation map

Defaults DSCP mutation map is not enabled on interface.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to apply a DSCP-to-COS mutation map defined by the **qos map dscp-mutation** *name* command to a specific interface.

Usage Guidelines The **qos dscp-mutation** *name* command applies a defined DSCP mutation map to the interface. Use the **no qos dscp-mutation** command while in the interface mode to remove the DSCP mutation map from the interface.

Examples To apply a configured qos dscp-mutation map named *test* to a specific interface, enter the **qos dscp-mutation** *name* command while in the interface mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# qos dscp-mutation test
```

To remove a configured qos dscp-mutation map named *test* from a specific interface, enter the **no qos dscp-mutation** *name* command while in the interface mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# no qos dscp-mutation
```

See Also **interface, qos map dscp-mutation**, show qos maps dscp-mutation

qos dscp-traffic-class

Applies a defined DSCP-to-Traffic-Class map to an interface,

Synopsis **qos dscp-traffic-class** *name*

no qos dscp-traffic-class

Operands *name* Name of DSCP-to-Traffic-Class map

Defaults DSCP-to-Traffic-Class map is not enabled on the interface.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to apply a qos DSCP-to-Traffic-Class map defined by the **qos map dscp-traffic-class** *name* command to a specific interface.

Usage Guidelines The **qos dscp-traffic-class** *name* command applies a defined map to the interface. Use the **no qos dscp-traffic-class** command while in the interface mode to remove the DSCP-to-Traffic-Class map from the interface.

Examples To apply a configured DSCP-Traffic-Class map named *test* to a specific interface, enter the **qos dscp-traffic-class** *name* while in the interface configuration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# qos dscp-traffic-class test
```

To remove a configured DSCP-Traffic-Class map named *test* from a specific interface, enter the **no qos dscp-traffic-class** command while in the interface configuration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# no qos dscp-traffic-class
```

See Also **interface, qos map dscp-traffic-class**, show qos maps dscp-traffic-class

qos flowcontrol tx

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 or deactivates the receiving portion of flow control.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description This command configures and activates QoS flow control.

When a 1Gbps local port is already online, and the **qos flowcontrol** command is issued, the pause settings take effect immediately on that local port. However, when the link is toggled, pause is re-negotiated. The local port will advertise the most recent **qos flowcontrol** settings. After auto completes, the local port pause settings may change, depending on the outcome of the pause negotiation, per 802.3 Clause 28B, as shown in Table 3.

TABLE 3 Pause negotiation results

Advertised LOCAL cfg	Advertised REMOTE cfg	Negotiated result
Rx=off Tx=on	Rx=on Tx=on	asymmetrical: LOCAL Tx=on --> pause --> REMOTE Rx=on
Rx=on Tx=on	Rx=off Tx=on	asymmetrical: LOCAL Rx=on <-- pause <-- REMOTE Tx=on
Rx=on Tx=n/a	Rx=on Tx=n/a	symmetrical : LOCAL Tx/Rx=on <-- pause --> REMOTE Tx/Rx=on
Rx=n/a Tx=n/a	Rx=off Tx=off	disable pause both sides

Usage Guidelines Use the **no qos flowcontrol** command to deactivate flow control on a specific interface.

Examples To activate both the transmitting and receiving portions of flow control on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-fo-1/3/1)# qos flowcontrol tx on rx on
```

To deactivate flow control on a specific port-channel interface:

```
switch(config)# interface Port-channel 33
switch(config-Port-channel-33)# no qos flowcontrol
```

See Also **interface**

qos flowcontrol pfc

Activates and configures flow control for a Class of Service (CoS).

Synopsis **qos flowcontrol pfc** *cos_value* **tx** [**on** | **off**] **rx** [**on** | **off**]

no qos flowcontrol pfc *cos_value*

Operands

cos_value	The CoS value.
tx [**on**	**off**]	Activates or deactivates the transmission portion of flow control.
rx [**on**	**off**]	Activates the receiving portion of flow control.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description In Brocade VCS Fabric mode, this command only affects per-interface pause behavior. To use flow control in Brocade VCS Fabric mode, use the CEE map configuration.

Usage Guidelines In Brocade VCS Fabric mode, this command only takes effect on the interface. In order to have PFC functionality through the Brocade VCS Fabric cluster, use the CEE map configuration.

Use the **no qos flowcontrol pfc** *cos_value* command to deactivate CoS flow control on a specific interface.

Examples To activate both the transmitting and receiving portions of a Class of Service (with a value of 7 in this example) flow control on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-fo-1/3/1)# qos flowcontrol pfc 7 tx on rx on
```

To deactivate both the transmitting and receiving portions of a Class of Service (with a value of 4 in this example) flow control on a specific port-channel interface:

```
switch(config)# interface Port-channel 33
switch(config-Port-channel-33)# no flowcontrol pfc 4
```

See Also interface

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 qos 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 QoS 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 **qos cos-mutation**, **show qos 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-Traffic Class QoS map does not exist, then it is created. If the named CoS-to-Traffic 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 None

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 **qos map cos-mutation**, **qos trust cos**

qos map dscp-cos

Creates a QoS map for performing DSCP-to-CoS mapping. This configures a DSCP-to-CoS map on the ingress interface.

Synopsis **qos map dscp-cos** *name*

no map dscp-cos *name*

mark *ingress dscp values* **to** *egress cos value*

Operands

name	Name of dscp-cos map
ingress dscp values	Range of input DSCP values
egress dscp values	Output CoS value

Defaults DSCP-to-CoS mutation is not enabled.

Command Modes dscp-cos mode for the qos map

Global configuration mode

Description Use this command to remap the incoming DSCP values of the ingress packet to egress CoS 802.1P values. When you launch the **qos map dscp-cos** command, the system is placed in dscp-cos mode for the configured map. At this point, you can map ingress DSCP values to egress CoS values using the **mark** command.

Usage Guidelines This command creates a qos dscp-cos map. Use the **no map dscp-cos** *name* command while in global configuration mode to remove the DSCP-CoS map. To apply the DSCP-CoS map to an interface, enter the **qos dscp-cos** *name* command while in configuration mode for a specific interface. To remove the map from the interface, enter the **no qos dscp-cos** *name* command while in the interface configuration mode.

Examples To create a QoS DSCP-CoS map and place system into dscp-cos mode:

```
switch(config)# qos map dscp-cos test
switch(dscp-cos-test)#
```

To map an ingress DSCP value to egress CoS values while in dscp-cos mode:

```
switch(dscp-cos-test)# mark 1,3,5,7 to 3
```

To map multiple ingress DSCP values to egress CoS values while in dscp-cos mode:

```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
switch(dscp-mutation-test)# mark 11,13,15,17 to 5
switch(dscp-mutation-test)# mark 12,14,16,18 to 6
switch(dscp-mutation-test)# mark 2,4,6,8 to 7
```

To remove a QoS DSCP-CoS map while in global configuration mode:

```
switch(config)# no qos map dscp-cos test
```

See Also **qos map dscp-traffic-class**, **qos dscp-cos**, **show qos maps dscp-cos**

qos map dscp-mutation

Creates a DSCP mutation by remapping the incoming DSCP value of the ingress packet to outgoing DSCP values.

Synopsis **qos map dscp-mutation** *name*

no map qos dscp-mutation *name*

mark *ingress dscp values* **to** *egress dscp value*

Operands

name	Name of dscp-mutation map
ingress dscp values	Range of input DSCP values
egress dscp values	Output DSCP value

Defaults DSCP mutation is not enabled.

Command Modes dscp-mutation mode for the dscp-mutation map

Global configuration mode

Description Use this command to remap the incoming DSCP values of the ingress packet to an egress DSCP value. When you launch the **qos map dscp-mutation** command, the system is placed in dscp-mutation mode for the configured map. At this point, you can map ingress DSCP values to egress DSCP values using the **mark** command.

Usage Guidelines This command creates a qos dscp-mutation map. Use the **no map dscp-mutation** *name* command while in global configuration mode to remove the dscp-mutation map. To apply the dscp-mutation map to an interface, enter the **qos dscp-mutation** *name* command while in configuration mode for a specific interface. To remove the map from the interface, enter the **no qos dscp-mutation** *name* command while in interface configuration mode.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To create a QoS DSCP-mutation map and place system into dscp-mutation mode:

```
switch(config)# qos map dscp-mutation test
switch(dscp-mutation-test)#
```

To map an ingress DSCP value to egress DSCP values while in dscp-mutation mode:

```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
```

To map multiple ingress DSCP values to egress DSCP values while in dscp-mutation mode:

```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
switch(dscp-mutation-test)# mark 11,13,15,17 to 19
switch(dscp-mutation-test)# mark 12,14,16,18 to 20
switch(dscp-mutation-test)# mark 2,4,6,8 to 10
```

To remove a QoS DSCP-mutation map while in global configuration mode:

```
switch(config)# no qos map dscp-mutation test
```

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

See Also show qos maps dscp-mutation, qos dscp-mutation

qos map dscp-traffic-class

Creates a QoS map for performing DSCP-to-Traffic Class mapping. This creates a dscp-traffic-class map on the ingress interface. You can configure an interface with either a DSCP-to-Traffic-Class map or a CoS-to-Traffic-Class map.

Synopsis

qos map dscp-traffic-class *name*

no qos map dscp-traffic-class *name*

mark *ingress dscp values* **to** *traffic class*

Operands

name	Name of QoS DSCP-to-Traffic Class map.
ingress dscp values	Range of input DSCP values
traffic class value	Traffic Class (0-7)

Defaults

DSCP-to-Traffic-Class mutation is not enabled.

Command Modes

dscp-traffic-class mode for the dscp-traffic-class map

Global configuration mode

Description

Use this command to remap the incoming DSCP values of the ingress packet to a Traffic Class. When you launch the **qos map dscp-traffic-class** command, the system is placed in dscp-traffic-class mode for the configured map. At this point, you can map ingress DSCP values to traffic class values using the **mark** command.

Usage Guidelines

This command creates a QoS DSCP-Traffic-Class map. Use the **no map dscp-mutation** *name* command to remove the map while in global configuration mode. To apply the QoS DSCP-Traffic-Class map to an interface, enter the **qos dscp-traffic-class** *name* command while in configuration mode for a specific interface. To remove the map from the interface, enter the **no qos dscp-traffic-class** *name* command while in the interface mode.

Examples

To create a QoS DSCP-Traffic-Class map and place system into dscp-traffic-class mode:

```
switch(config)# qos map dscp-traffic-class test
switch(dscp-traffic-class-test)#
```

To map ingress DSCP values to a traffic class while in dscp-traffic-class mode:

```
switch(dscp-traffic-class-test)# mark 1,3,5,7 to 3
```

To map multiple ingress DSCP values to traffic classes while in dscp-traffic-class mode:

```
switch(dscp-traffic-class-test)# mark 1,3,5,7 to 3
switch(dscp-traffic-class-test)# mark 11,13,15,17 to 5
switch(dscp-traffic-class-test)# mark 12,14,16,18 to 6
switch(dscp-traffic-class-test)# mark 2,4,6,8 to 7
```

To remove a QoS DSCP-Traffic-Class map while in global configuration mode:

```
switch(config)# no qos map dscp-traffic-class test
```

See Also

show qos maps dscp-traffic-class, **qos dscp-traffic-class**

qos red profile

Creates a Random Early Discard (RED) profile for egress traffic flow.

Synopsis **qos red-profile** *profile-ID value* **min-threshold** *percentage* **max-threshold** *percentage* **drop-probability** *percentage*

no qos red-profile *profile-ID*

Operands

profile-ID value	Value from 1 through 384
percentage	0-100%
min-threshold	Minimum threshold (percentage) of queue size (0 through 100) for randomly dropping packets.
max-threshold	Maximum threshold (percentage) of queue size (0 through 100) when packets are dropped with 100% probability.
drop-probability	Probability that packets will be dropped when minimum threshold is reached.

Defaults none

Command Modes Global configuration mode

Description Configure a Random Early Discard (RED) profile with the **qos red-profile** command and provide a minimum threshold, maximum threshold, and drop-probability.

Usage Guidelines This command creates a RED profile for egress traffic flow. Enter **no qos red-profile** *profile-ID* to remove the profile while in global configuration mode. To map the profile to a CoS priority for a port, enter the **qos random-detect cos** command while in configuration mode for a specific interface. To remove the profile from the interface, enter the **no qos random-detect cos** command while in the interface mode. You must remove the profile from interface before you can remove the profile itself.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To create a RED profile while in global configuration mode:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# qos red-profile 2 min-threshold 10 max-threshold 80
drop-probability 80
```

To remove the profile while in global configuration mode:

```
switch(config)# no qos red-profile 2
```

See Also **show qos red profiles, qos random-detect cos**

qos trust cos

Specifies the interface QoS trust Class of Service (CoS) 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 subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to specify the interface ingress QoS trust CoS 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.

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.

Use the **no qos trust cos** command to return to the default.

Examples To set the interface QoS to the CoS trust mode for a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos trust cos
```

To return the interface QoS to the default value or to the untrusted state:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# 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 **interface qos cos, show qos maps**

qos trust dscp

Enables Differentiated Services Code Point (DSCP) mode for incoming traffic.

Synopsis **qos trust dscp**

no qos trust dscp

Operands None

Defaults The QoS trust DSCP mode set to the untrusted state.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to specify the interface ingress QoS trust DSCP mode, which controls user priority mapping of incoming traffic. The untrusted mode overrides all incoming priority markings with the Interface Default CoS. The DSCP trust mode sets the user priority based on the incoming DSCP value, When this feature is not enabled, DSCP values in the packet are ignored.

When DSCP trust is enabled, the Table 4 lists the default mapping of DSCP values to user priority.

TABLE 4 Default DSCP priority mapping

DSCP Values	User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Usage Guidelines QoS Trust Mode is automatically applied if dscp-cos map or qos dscp traffic class is applied to the interface.

Use the **no qos trust dscp** command to return to the default.

Examples To set the interface QoS to DCSP trust mode on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos trust dscp
```

To return the interface QoS to the default value or to the untrusted state:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no qos trust dscp
```

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

See Also **interface, qos map dscp-cos, qos map dscp-traffic-class, show qos interface, show qos maps dscp-traffic-class**

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 qos queue multicast scheduler

Operands

dwrr	Configures the DWRR multicast Traffic Class packet expansion policy.
mTC0_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 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 qos queue multicast scheduler** command to return the multicast Traffic Class packet expansion scheduler to the default value.

Usage Guidelines None

Examples To set the multicast Traffic Class packet expansion scheduler for Traffic Class 0 getting 5 percent bandwidth, Traffic Class 1 getting 10 percent bandwidth, Traffic Class 2 getting 15 percent bandwidth, and Traffic Class 3 getting 20 percent bandwidth, and so on:

```
switch(config)#qos queue multicast scheduler dwrr 5 10 15 20 5 10 15 20
```

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.

weight7 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 Brocade VCS Fabric 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 cos-threshold

Configures the port tail drop thresholds.

Synopsis **qos rcv-queue cos-threshold** *TDT0* {*TDT1* | *TDT2* | *TDT3* | *TDT4* | *TDT5* | *TDT6* | *TDT7*}

no qos rcv-queue cos-threshold

Operands

TDT0	Defines the proportion for the first port tail drop threshold. The range of valid values is from 0 through 100.
TDT1	Defines the proportion for the second port tail drop threshold. The range of valid values is from 0 through 100.
TDT2	Defines the proportion for the third port tail drop threshold. The range of valid values is from 0 through 100.
TDT3	Defines the proportion for the fourth port tail drop threshold. The range of valid values is from 0 through 100.
TDT4	Defines the proportionfor the fifth port tail drop threshold. The range of valid values is from 0 through 100.
TDT5	Defines the proportion for the sixth port tail drop threshold. The range of valid values is from 0 through 100.
TDT6	Defines the proportion for the seventh port tail drop threshold. The range of valid values is from 0 through 100.
TDT7	Defines the proportion for the eighth port tail drop threshold. The range of valid values is from 0 through 100.

Defaults None

Command Modes Interface subconfiguration mode (gi, te).

Description Every port has associated with it a total of 9 CoS thresholds, one for the port tail drop threshold and the other eight are thresholds for per priority. To give a fair allocation of buffers for the traffic from all priorities, the port buffers are allocated among different priorities. That is achieved through per priority tail drop thresholds. The port tail drop threshold represents the amount of buffers given to the port and per priority tail drop thresholds (CoS tail drop thresholds from now on) represents the buffers allocated to each CoS.

Whenever the buffers allocated to a priority are fully exhausted, all the traffic coming in on that priority is dropped. In the absence of per priority tail drop thresholds (and only port tail drop threshold), the buffers would be consumed on a first come first serve basis and results in an unfair share of buffers between all the priorities. If you know which priority traffic is most seen, then giving good number of buffers for those priorities results in less number of packet drops for those priorities.

Therefore, instead of using the standard priority values, you can assign anywhere from 0% through 100% priority to any threshold, with the sum value of all eight priorities not to exceed 100%.

For example, using the priorities 5 5 5 5 50 20 2 8 sums up to 100%.

Usage Guidelines The tail drop thresholds are not allowed to exceed 100%, but can be below 100%. For example, if the tail drop thresholds entered are less than 100%, then the buffer allocation happens as per what has been configured.

Use the **no qos rcv-queue cos-threshold** command to remove the configured tail drop thresholds .

Examples

```
switch (config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos rcv-queue cos-threshold 5 5 5 5 50 20 2 8
switch(conf-if-te-178/0/9)# do show qos in te 178/0/9
Interface TenGigabitEthernet 178/0/9
CoS-to-Traffic Class map 'default‘
               In-CoS:   0   1   2   3   4   5   6   7
  ------------------------------------------------
  Out-CoS/TrafficClass: 0/1 1/0 2/2 3/3 4/4 5/5 6/6 7/7
Per-Traffic Class Tail Drop Threshold (bytes)
         TC:      0      1      2      3      4      5      6      7
  ------------------------------------------------------------------
  Threshold:  10180  10180  10180  10180 101808  40723   4072  16289
```

See Also interface, qos rcv-queue multicast threshold

qos random-detect cos

Maps a RED profile to a CoS priority value for a port,

Synopsis **qos random-detect cos** *value* **red-profile-id** *profile-ID value*

no qos random-detect cos *value*

Operands

value	Class of Service (COS) value from 0-7.
red-profile-id	Value from 1 through 384

Defaults Port CoS priority value not mapped to RED profile.

Command Modes Interface subconfiguration mode (fo, gi, Port-channel, te).

Description Use this command to map a RED profile to a CoS priority value for a specific interface. The RED profile is defined by the **qos red-profile** command.

Usage Guidelines The **qos random-detect** command maps a RED profile to a CoS value for a specific interface. Use the **no qos random-detect cos** *value* command while in the interface mode to remove the DSCP-to-Traffic-Class map from the interface.

Examples To map the profile to CoS priority 7 on the tengigabitethernet interface 1/2/2:

```
switch(config)# interface tengigabitethernet 1/2/2
switch(conf-if-te-1/2/2)# qos random-detect cos 7 red-profile-id 2
```

To remove the above profile from interface 1/2/2:

```
switch(config)# interface tengigabitethernet 1/2/2
switch(conf-if-te-1/2/2)# no qos random-detect cos 7
```

See Also **interface, qos red profile, show qos red profiles, show qos red statistics interface**

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 None This command is not supported on VDX 8770-4 and VDX 8770-8 platforms.

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

Configures a cap on the maximum queue depth for multicast packet expansion queues.

Synopsis **qos rcv-queue multicast threshold** *mTC0 mTC1 mTC2 mTC3 mTC4 mTC5 mTC6 mTC7*

no qos rcv-queue multicast threshold

Operands

mTC0	Sets the Tail Drop Threshold for multicast Traffic Class 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.

Defaults The default is 64 packets for each multicast Traffic Class.

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 queues to the default value.

Usage Guidelines None This command is not supported on VDX 8770-4 and VDX 8770-8 platforms.

Examples To increase multicast packet expansion Tail Drop Threshold to 1000 pkt for each multicast Traffic Class:

```
switch(config)# qos rcv-queue multicast threshold 1000 1000 1000 1000 1000 1000
1000 1000
```

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-profile (AMPP)

Activates the QoS profile mode for AMPP.

Synopsis **qos-profile**

no qos-profile

Operands None

Defaults None

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 Use the **no qos-profile** command to remove the profile.

Examples

```
switch(config)# port-profile sample-profile
switch(conf-pp)# qos-profile
```

See Also None

radius-server

Configures the Remote Authentication Dial-In User Service (RADIUS) server.

Synopsis **radius-server host** {*ip-address* | *host_name*} [**auth-port** *portnum*] [**protocol** {**chap**|**pap** |**peap**}] [**key** *shared_secret*] [**timeout** *sec*] [**retries** *num*]

no radius-server host *hostname*| *ip-address*

Operands

host {*ipaddr* | *host_name*}
Specifies the IP address or host name of the RADIUS server. IPv4 and IPv6 addresses are supported. The maximum supported length for the RADIUS hostname is 40 characters.

auth-port *port*
Specifies the user datagram protocol (UDP) port used to connect the RADIUS server for authentication. The valid range is 0 through 65535. The default port is 1812.

protocol {**chap** | **pap** | **peap**}
Specifies the authentication protocol. Options include CHAP, PAP, or PEAP-MSCHAP. The default is CHAP.

key *shared_secret*
The text string that is used as the shared secret between the switch and the RADIUS server. The default is **sharedsecret**. The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the shared secret string in either double quotation marks or use the escape character (\) as shown in the example: **"secret!key"** or **secret\!key**.

timeout *sec*
The time to wait for the RADIUS server to respond, in seconds. The default is 5 seconds.

retries *num*
The number of attempts allowed to connect to a RADIUS server. The default is 5 attempts.

Defaults The following are the default values of the RADIUS server 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 The key operand does not support an empty string.

Use this command to configure the attributes of the RADIUS server. If a RADIUS server with the specified IP address or host name does not exist, it is added to the server list. If the RADIUS server already exists, this command modifies the configuration.

Usage Guidelines The **no** form of the **radius-server** command resets the specified parameters to their default values.

Examples To configure a RADIUS server:

```
switch(config)# radius-server host 10.24.65.6 protocol chap retransmit 100
switch(config-radius-server-10.24.65.6)#
```

To modify the previously configured RADIUS server:

```
switch(config)# radius-server host 10.24.65.6 protocol pap key
“new#radius*secret timeout 10
```

To reset the timeout value to the default:

```
switch(config)# no radius-server host 10.24.65.6 timeout
```

See Also show running-config radius-server, show running-config tacacs-server, tacacs-server

rate-limit-delay get netconf

Returns the rate limit delay configured for processing NETCONF Remote Procedure Calls (RPCs).

Synopsis **debug internal rate-limit-delay get netconf**

Operands None

Defaults None

Command Modes privileged EXEC mode

Description This command returns the configured minimum time in milliseconds between processing successive NETCONF RPCs. A value of zero indicates that RPC processing is unlimited.

Usage Guidelines None

Examples None

See Also **rate-limit-delay set netconf**

rate-limit-delay set netconf

Limits the rate at which BNA or NETCONF Remote Procedure Call (RPC) requests can be processed on the switch.

Synopsis **debug internal rate-limit-delay set netconf** *delay*

Operands *delay* The number of milliseconds the system waits between processing RPCs.

Defaults 0—The RPC processing rate is unlimited.

Command Modes Privileged EXEC mode

Description This command limits the rate at which RPCs can be processed on the switch by specifying the minimum delay between processing successive RPCs.

Usage Guidelines Use this command to prevent excessive numbers of RPCs from adversely affecting switch performance.

Examples The following example limits the processing of RPCs to a maximum of one every 50 milliseconds.

```
switch# debug internal rate-limit-delay set netconf 50
```

See Also **rate-limit-delay get netconf**

redistribute

Enables route redistribution.

Synopsis **redistribute** {**connected** | **static**} [**route-map** *string*]

Operands

connected	Enables redistribution of connected routes into OSPF.
static	Enables redistribution of static routes into OSPF.
route-map string	Route-map to filter routes being redistributed.

Default None

Command Modes Router configuration mode.

Description Enables route redistribution in OSPF. The routes are imported into OSPF from the routing table manager. If a route-map is specified, only those routes that pass the filter are imported. The routes are then redistributed to neighbors by Type 4 or Type 5 LSAs.

For an external route that is redistributed into OSPF through a route map, the metric value of the route remains the same unless the metric is set by a set metric command inside the route map. The **default-metric** command has no effect on the route. This behavior is different from a route that is redistributed without using a route map. For a route redistributed without using a route map, the metric is set by the **default-metric** command.

Usage Guidelines You must configure the route map before you configure a redistribution that uses the route map.

When you use a route map for route redistribution, the software disregards the permit or deny action of the route map.

Use the **no** parameter to disable route redistribution.

Examples To import all connected routes into OSPF that pass the filters specified in the already configured route map called *myroutemap*:

```
switch(conf-ospf-router)# redistribute connected route-map myroutemap
```

See Also **default-metric**

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 **None**

Command Modes Protocol Spanning Tree MSTP mode

Description Use this command to assign a name to an MSTP region.

Usage Guidelines Use the **no region** command to delete the name.

The *region-name* string has a maximum length of 32 characters and is case-sensitive.

This command functions only in standalone mode.

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) or management module.

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 or management module.

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.

On a compact switch, If the power-on-self-test(POST) is enabled, it is executed when the system comes back up.

On a modular chassis, the **reload** commands only reboots the management module on which the command is executed. If you log in to the switch IP address and execute the reload command, only the active management module reboots and POST is bypassed.

Examples To perform a cold reboot on the switch:

```
switch# reload

Warning: Unsaved configuration will be lost. Please run `copy running-config
startup-config` to save the current configuration if not done already.

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

See Also **fastboot**

remap fabric-priority

Remaps the CoS fabric priority.

Synopsis **remap fabric-priority** *priority*

Operands

priority	Specifies the remapped CoS priority value for Brocade VCS Fabric mode. The range of valid values is from 0 through 6.

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 Brocade VCS Fabric mode.

Usage Guidelines None

Examples None

See Also None

remap lossless-priority

Remaps the Brocade VCS Fabric priority.

Synopsis **remap lossless-priority** *priority*

Operands

priority	Specifies the remapped priority value. The range of valid values is from 0 through 6.

Defaults The default value is 0.

Command Modes CEE map configuration mode

Description This command remaps the Brocade VCS Fabric lossless priorities to a different priority.

Usage Guidelines None

Examples None

See Also None

rename

Renames a file in the switch flash memory.

Synopsis **rename** *current_name new_name*

Operands

current_name	The file name you wish to change.
new_name	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
drwxr-xr-x   2 root     sys          4096 Feb 13 00:39 .
drwxr-xr-x   3 root     root         4096 Jan  1  1970 ..
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 myconfig.old
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x   1 root     sys           697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--   1 root     root         6800 Feb 13 00:37 startup-config
```

See Also copy, delete, dir, show file

resequence

Specifies the renumbering of the rules in a MAC or IP ACL.

Synopsis **resequence** {**ip** | **mac**} **access-list** *name* [*seq_num* | *increment*]

Operands

ip | **mac**	Specifies whether to access an IP or MAC ACL.
name	Specifies the name of a standard or an extended ACL.
seq_num	Specifies the starting sequence number in the 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 None

Command Modes Privileged EXEC mode

Description Use this command to reassign sequence numbers to entries of an existing MAC or IP access-list.

Usage Guidelines Reordering the sequence numbers is useful when you need to insert rules into an existing MAC or IP 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 (extended MAC ACLs), seq (standard IP ACLs), seq (standard MAC ACLs)**

reserved-vlan

Defines the range of VLANs that cannot be created using the **interface vlan** command.

Synopsis **reserved-vlan** *start-VLAN-ID end-VLAN-ID*

Operands

start-VLAN-ID	The range of valid values is any positive number below 4090.
end-VLAN-ID	The range of valid values is any positive number below 4090.

Defaults For the Brocade VDX 6720, the default reserved space is 128 VLANS, and is equal to sum of the number of maximum allowed portchannels and the number of interfaces in the Brocade VDX 6720-60 switch. Presently, VLANs from 3960 through 4090 are reserved by default.

For Brocade VDX 8770, the default reserved VLAN space is 4. Presently, VLANs from 4087 through 4090 are reserved by default.

Command Modes Global configuration mode

Description This command defines the range of VLANs that cannot be created using the **interface vlan** command.

Usage Guidelines This command succeeds if there are no wired VLANs configured in the specified range. Otherwise, an error instructs you to delete the wired VLANs in the specified range, or provide a different range.

VLAN 1002 is still the default FCoE VLAN. VLAN 1002 cannot be part of the reserved VLAN range unless some other VLAN is created for FCoE.

This command does not require a switch reboot.

Examples None

See Also **show default-vlan, show running reserved-vlan**

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 This command functions only in standalone mode.

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**

rfc1583-compatibility

Configures compatibility with RFC 1583.

Synopsis **rfc1583-compatibility**

Operands This command has no operands.

Default OSPF is compatible with RFC 1583 (OSPFv2).

Command Modes Router configuration mode.

Description Enables or disables compatibility with RFC 1583. By default, OSPF is compatible with RFC 1583 (OSPFv2) and therefore maintains a single best route to an autonomous system (AS) boundary router in the OSPF routing table. Disabling this compatibility causes the OSPF routing table to maintain multiple intra-AS paths, which helps prevent routing loops.

Usage Guidelines Use the **no** parameter to disable compatibility with RFC 1583.

Examples To disable compatibility with RFC 1583:

```
switch(conf-ospf-router)# rfc1583-compatibility
```

rfc1587-compatibility

Configures compatibility with RFC 1587.

Synopsis **rfc1587-compatibility**

Operands **This command has no operands.**

Default OSPF is compatible with RFC 1587 (OSPFv2).

Command Modes Router configuration mode.

Description Enables or disables compliance with RFC 1587, the original NSSA specification. Only part of the newer RFC 3101 is supported—the "no-summary" option and the handling of default-route LSAs when "no summary" is enabled.

Usage Guidelines Use the **no** parameter to disable compatibility with RFC 1587.

Examples To disable compatibility with RFC 1587:

```
switch(conf-ospf-router)# no rfc1587-compatibility
```

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 None

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 Ethernet group statistics for later retrieval.

Synopsis **rmon collection history** *number* [**buckets** *bucket_number* | **interval** *seconds* | **owner** *name*]

no romn collection history *number*

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 3600. The default value is 1800.
owner *name*	Specifies the identity of the owner. The maximum number of characters is 15.

Defaults The collection of RMON history is not enabled.

Command Modes Interface subconfiguration mode (fo, i, te).

Description Use this command to collect periodic statistical samples of Ethernet group statistics on a specific interface for later retrieval.

Usage Guidelines Use the **no rmon collection history** *number* command to disable the history of statistics collection.

Examples To collect RMON statistics, with an RMON collection control index value of 5 for the owner named *admin*, on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 170/0/1
switch(conf-if-te-170/0/1)# rmon collection history 5 owner admin
```

See Also **interface**, **show rmon history**

rmon collection stats

Collects Ethernet group statistics.

Synopsis **rmon collection stats** *number* [**owner** *name*]

no rmon collection stats *number*

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 subconfiguration mode (fo, i, te).

Description Use this command to collect Ethernet group statistics on a specific interface.

Usage Guidelines Use the **no rmon collection stats** *number* command to disable the collection of statistics.

Examples To collect RMON statistics, with an RMON collection control index value of 2 for the owner named *admin*, on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 170/0/1
switch(conf-if-te-170/0/1)# rmon collection stats 2 owner admin
```

See Also interface, 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 None

Examples To configure an RMON event:

```
switch(config)# rmon event 2 log description “My Errorstoday” owner gjack
```

See Also **show rmon history**

role

Creates or modifies a user role.

Synopsis **role name** *role_name* [**desc** *description*]

no role name

Operands

name *role_name*	The name of the role.
desc *description*	An optional description of the role.

Defaults None

Command Modes Global configuration mode

Description Use this command to create a new role. A role defines the access privileges of the user accounts on the switch. A user is associated with a single role. You first create the role and later associate the role with rules to define the access permissions.

Usage Guidelines The role name must begin with a letter and can contain alphanumeric characters and underscores. The length of the role name should be between 4 and 32 characters. The name cannot be same as that of an existing user.

The description field supports up to 64 characters and can include any printable ASCII character, except for the following characters: single quotation marks (‘), double quotation marks(“), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces. you must enclose the text in double quotation marks.

The maximum number of roles supported is 64.

Using the **no** form of the role command sets the attributes to their default values.

Examples To create a role of a VCS administrator

```
switch(config)# role name VCSAdmin desc “Manages VCS fabrics”
```

To reset the description to the default value (no description):

```
switch(config)# no role name VCSAdmin desc
```

To delete the role:

```
switch(config)# no role name VCSAdmin desc
```

See Also **rule, show running-config role, show running-config rule**

route-map

Creates or deletes a route map instance.

Synopsis **route-map** *name* [**permit** | **deny**] *instance_id*

no route-map *name*

Operands

name	The name of the route map. The operand can be up to 63 ASCII characters in length.
permit	Creates the map.
deny	Deletes the map.
instance_id	The instance ID. The range of valid values is from 1 through 65535.

Defaults None

Command Modes Privileged EXEC mode

Description This command creates or deletes a route map instance.

Usage Guidelines The maximum number of OSPF networks that can be advertised and processed in a single area in a router is limited to 600.

Examples None

See Also **ip prefix-list**, **match interface**, **match ip address**, **match ip next-hop**, **match metric**, **match route-type**, **match tag**, **route-map**, **set distance**, **set ip next-hop**, **set metric**, **set tag**

router ospf

Enables the OSPF routing protocol.

Synopsis **router ospf**

Operands None

Default Enabled.

Command Modes Configuration mode.

Description Enables the OSPF routing protocol and enter OSPF router configuration mode.

Usage Guidelines Use the **no** option to delete all current OSPF configuration and to block any further OSPF configuration.

Examples To enable the OSPF routing protocol:

```
switch(config)# router ospf
```

rule

A rule defines the permissions applicable to a particular role.

Synopsis **rule** *index* [**action** {**accept** | **reject**}] [**operation** {**read-only** | **read-write**}] **role** *role_name* **command** *command_name*

no rule *index*

Operands

index Specifies a numeric identifier for the rule. The valid range is from 1 through 512.

action accept | **reject**
Specifies whether the user is accepted or rejected while attempting to execute the specified command. Accept is the default value.

operation read-only | **read-write**
Specifies the type of operation permitted. **Read-write** is the default.

role *role_name* Specifies the name of the role for which the rule is defined.

command *command_name*
Specifies the command for which access is defined. Separate commands options by a space. RBAC support is provided only for the following commands with options: copy, clear, interface, and protocol.

Defaults Refer to the operand section.

Command Modes Global configuration mode

Description Use this command to create the Role-Based Access Permissions (RBAC) permissions associated with a role. Network OS uses RBAC as the authorization mechanism. Every user account must be associated with a role. Every user account can only be associated with a single role. Note that the permissions cannot be assigned directly to the user accounts and can only be acquired through the associated role.

Usage Guidelines When you create a rule, the **role**, index, and **command** operands are mandatory and the **action** and **operation** operands are optional. The maximum number of rules is 512.

When you modify a rule, all operands except **index** are optional.

Examples To create a rule allowing the NetworkSecurityAdmin role to create user accounts:

```
switch(config)# rule 150 action accept operation read-write role
NetworkSecurityAdmin command config

switch(config)# rule 155 action accept operation read-write role
NetworkSecurityAdmin command username
```

To delete a rule:

```
switch(config)# no rule 155
```

See Also **role, show running-config role, show running-config rule**

secpolicy activate

Activates the defined switch connection control (SCC) policy and its member set.

Synopsis **secpolicy activate**

Operands None

Defaults By default, any switch is allowed to join the fabric; the SCC policy does not exist until it is defined and activated.

Command Modes Privileged EXEC mode

Description This command activates the defined SCC policy and its member set. The SCC policy is used to restrict which switches can join the fabric by either accepting or rejecting the connection between two switches. Switches are checked against the policy each time an E_Port-to-EX_Port connection is made. The policy is named SCC_POLICY and accepts device members listed as World Wide Names (WWNs).

Usage Guidelines Although the **active-policy** is listed under the possible completions of **secpolicy** command, the **defined-policy** option should be used to create or add policy or members,. The secpolicy activate command activates the policy.

A defined SCC policy must exist before you can activate the policy. You create the policy with the **secpolicy defined-policy** command..

During configuration replay, the defined and active policies are replayed and the E_Ports are enabled or disabled based on the SCC policy entries in the active policy list.

During **copy file running-config** command execution, only the defined policy in the switch is updated with the config file entries; the active policy entries remain unchanged. In this case, you must use the **secpolicy activate** command to activate the defined policy list.

This command is supported only on the Brocade VDX 6730 platforms.

Examples To activate the defined SCC policy:

```
switch# secpolicy activate
```

See Also **secpolicy defined-policy, show running-config role**

secpolicy defined-policy

Creates the switch connection control (SCC) policy and adds the SCC defined policy set members (WWNs).

Synopsis **secpolicy defined-policy SCC_POLICY** [**member-entry** *switch_wwn*]

no secpolicy defined-policy SCC_POLICY [**member-entry** *switch_wwn*]

Operands **member-entry** *switch_wwn*
The switch WWN to be added to the SCC defined policy set.

Defaults By default, any switch is allowed to join the fabric; the SCC policy does not exist until it is created.

Command Modes Global configuration mode

Description Use this command to create the defined SCC policy or to modify an existing SCC policy by adding add policy set members (switch WWNs). When you execute this command, the SCC policy entry is created (if not present) and the WWNs are added to the SCC policy.

The SCC policy defines which switches can join the fabric by either accepting or rejecting the connection between two switches. Switches are checked against the policy each time an E_Port-to-EX_Port connection is made. The policy is named SCC_POLICY and accepts members listed as WWNs.

Usage Guidelines Although the **active-policy** is listed under the possible completions of **secpolicy** command, the defined-policy option should be used to create or add policy or members,. The **secpolicy activate** command activates the policy.

You can add multiple WWNs separated by a comma.

Use the **no secpolicy defined-policy SCC_POLICY member-entry** *switch_wwn* command to remove a switch (WWN) from the defined policy member set.

Use the **no secpolicy defined-policy SCC_POLICY** command to remove the SCC policy, along with all of the defined policy members.

After you configure the defined SCC_POLICY, execute the **secpolicy activate** command to apply the changes to the active policy set.

This command is supported only on the Brocade VDX 6730 platforms.

Examples To create the defined SCC policy:

```
switch(config)# secpolicy defined-policy SCC_POLICY
```

To add a switch WWN to the policy set:

```
switch(config)# secpolicy defined-policy SCC_POLICY member-entry \
    10:00:00:05:1e:00:69:00
```

To remove an entry from the policy set:

```
switch(config)# no secpolicy defined-policy SCC_POLICY member-entry \
    10:00:00:05:1e:00:69:00
```

To remove the SCC_POLICY entry

```
switch(config)# no secpolicy defined-policy SCC_POLICY
```

See Also **secpolicy activate, show running-config role**

security-profile (AMPP)

Activates the security-profile mode for AMPP.

Synopsis **security-profile**

no security-profile

Operands None

Defaults None

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 Use the **no security-profile** command to remove the profile.

Examples

```
switch(config)# port-profile sample-profile
switch(conf-pp)# security-profile
```

See Also None

seq (extended IP ACLs)

Inserts a rule anywhere in the IP ACL.

Synopsis

seq *value* [**deny** | **permit** | **hard-drop**] *ip-protocol* [**any** | **host** *Source_IP_ADDRESS*| *Source_IP_mask*] [*source_port_number* {**eq** | **gt** | **lt** | **neq** | **range**}] {**any** | *Destination_IP mask* | **host** *Destination_IP*} [{**eq** | **gt** | **lt** | **neq** | **range**} *destport-number*] [**dscp** *value*] [**ack fin rst sync urg psh**] [**count**] [**log**] [**remark** *comment*]

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.

hard-drop Drops the packet absolutely and can override the control packet trap entries, but does not override the permit entry that occurs before this rule in the ACL.

ip-protocol Indicates the type of IP packet you are filtering. You can specify a well-known name for any protocol whose number is less than 255, otherwise any decimal number may be entered.

any Specifies any source IP address.

host *Source_IP_ADDRESS*
Specifies the source host IP address for which to set permit or deny conditions.

Source_IP_mask Specifies the source host IP address for which to set permit or deny conditions. The address can also be entered as an IP address, or an IP address with a mask. The mask value can be entered in Classless Interdomain Routing (CIDR) format, or in wildcard mask format. For example, the following to entries yield the same results. The CIDR equivalent of “209.157.22.26 0.0.0.255” is “209.157.22.26/24”. In wildcard format, you can mask for any bit. For example, 0.255.0.255 is valid.

source_port_number This field is only valid when the ip-protocol has been specified as UDP or TCP. The keyword “operator” defines how to apply the sport number(s) that follow.

eq The policy applies to the TCP or UDP port name or number you enter after **eq**.

gt The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt**.

lt The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt**.

neq The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

range The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53. The first port number in the range must be lower than the last number in the range.

any Applies to all IP addresses received. The address can also be entered as an IP address along with a mask. The mask value can be entered in Classless Interdomain Routing (CIDR) format or in wildcard mask format. For example, the following to entries yield the same results. The CIDR equivalent of “209.157.22.26 0.0.0.255” is “209.157.22.26/24”. In wildcard format the user is free to mask for any bit ie 0.255.0.255 is valid.

Destination_ip mask
Specifies the destination host IP address for which to set permit or deny conditions. The address can also be entered as an IP address, or an IP address with a mask. The mask value can be entered in Classless Interdomain Routing (CIDR) format, or in wildcard mask format. For example, the following to entries yield the same results. The CIDR equivalent of “209.157.22.26 0.0.0.255” is “209.157.22.26/24”. In wildcard format, you can mask for any bit. For example, 0.255.0.255 is valid.

host *Destination_ip*
If only a single IP address is required for the filter it can be specified using the “host” keyword along with the source IP address.

eq The policy applies to the TCP or UDP port name or number you enter after **eq**.

gt The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt**.

lt The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt**.

neq The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

dscp *value* Matches the specified “value” against the DSCP value of the received packet. The range of valid values is from 0 through 63.

ack fin rst sync, **urg**, **psh**
Any combination of these TCP flags may be specified.

count Enables ACL hit accounting on the associated filter.

log Packets matching the filter are sent to the CPU and a corresponding log entry is generated by enabling the logging mechanism. This option is only available with permit and deny.

remark *comment* An ASCII string, up to 256 characters in length.

Defaults By default, no IP ACLs are configured.

Command Modes Feature Access Control List configuration mode

Description Use this command to insert a rule anywhere in the IP ACL; it configures rules to match and permits or drops traffic based on the source and destination IP 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 IP ACL.

Usage Guidelines The first set of [**any** | **host** *Source_IP_ADDRESS* | *Source_IP_ADDRESS*] parameters is specific to the source IP address. The second set of [**any** | **host** *Destination_IP_ADDRESS* | *Destination_IP_ADDRESS*] parameters is specific to the destination IP address.

Examples None

See Also **seq (standard IP ACLs)**

seq (standard IP ACLs)

Inserts a rule anywhere in the IP ACL.

Synopsis **seq** *value* [**deny** | **permit** | **hard-drop**] [**any** | **host** *SIP_address*| *SIP_address mask*] [**count**] [**log**] [**remark** *comment*]

no seq *value*

Operands

value	Specifies the sequence number for the rule. The range of valid values is from 0 through 4294967290.
permit	Specifies rules to permit traffic.
deny	Specifies rules to deny traffic.
hard-drop	Drops the packet absolutely and can override the control packet trap entries, but does not override the permit entry that occurs before this rule in the ACL.
any	Specifies any source MAC or IP address.
host *SIP_address*	Specifies the source host IP address for which to set permit or deny conditions.
SIP_mask	Specifies the destination host IP address for which to set permit or deny conditions. The address can also be entered as an IP address, or an IP address with a mask. The mask value can be entered in Classless Interdomain Routing (CIDR) format, or in wildcard mask format. For example, the following to entries yield the same results. The CIDR equivalent of “209.157.22.26 0.0.0.255” is “209.157.22.26/24”. In wildcard format, you can mask for any bit. For example, 0.255.0.255 is valid.
count	Enables the counting of the packets matching the rule.
log	Packets matching the filter are sent to the CPU and a corresponding log entry is generated by enabling the logging mechanism. This option is only available with permit and deny.
remark *comment*	An ASCII string, up to 256 characters in length.

Defaults By default, no IP 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 IP 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 IP ACL.

Usage Guidelines None

Examples None

See Also **seq (extended MAC ACLs)**

seq (extended MAC ACLs)

Inserts a rule anywhere in the MAC ACL.

Synopsis **seq** *value* [**deny** | **permit**] [**any** | **host** *MAC_ADDRESS*| *MAC_ADDRESS*] [**any** | **host** *MAC_ADDRESS*| *MAC_ADDRESS*] [*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_ADDRESS*	Specifies the source host MAC address for which to set permit or deny conditions. Use the format HHHH.HHHH.HHHH.
MAC_ADDRESS	Specifies the destination host MAC address for which to set permit or deny conditions. Use the format HHHH.HHHH.HHHH.
any	Specifies any destination MAC address.
host *MAC_ADDRESS*	Specifies the source host address for which to set permit or deny conditions. Use the format HHHH.HHHH.HHHH.
MAC_ADDRESS	Specifies the destination host address for which to set permit or deny conditions. Use the format HHHH.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_ADDRESS* | *MAC_ADDRESS*] parameters is specific to the source MAC address. The second set of [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] 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), permit (extended ACLs), permit (standard ACLs), resequence

seq (standard MAC ACLs)

Inserts a rule anywhere in the MAC ACL.

Synopsis **seq** *value* [**deny** | **permit**] [**any** | **host** *MAC_ADDRESS*| *MAC_ADDRESS*] [**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_ADDRESS*	Specifies the source host MAC address for which to set permit or deny conditions. Use the format HHHH.HHHH.HHHH.
MAC_ADDRESS	Specifies the destination host MAC address for which to set permit or deny conditions. Use the format HHHH.HHHH.HHHH.
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 None

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), permit (extended ACLs), permit (standard ACLs), resequence**

service password-encryption

Enables or disables password encryption.

Synopsis **service password-encryption**

no service password-encryption

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to enable encryption for all user account passwords.

Usage Guidelines The **no service password-encryption** command disables password encryption.

Examples To enable password encryption:

```
switch(config)# service password-encryption
```

To disable password encryption:

```
switch(config)# no service password-encryption
```

See Also **password-attributes, show running-config password-attributes**

service-policy

Binds a policy-map to an interface.

Synopsis **service-policy in** | **out** *policy-map name*

no service-policy in | **out**

Operands

in	Binds policy-map to inbound traffic.
out	Binds policy-map to outbound traffic.
policy-map name	Name of police policy-map

Defaults No created service policy.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description Use this command to apply a police policy-map to an interface. The policy-map must be configured before you can apply it (refer to "policy-map" on page 311).

Usage Guidelines This command applies a policy-map containing a class-map with specific Policer parameters and match critters to a switch interface. Use the **no service-policy in** | **out** command while in the applicable interface subconfiguration mode to remove the service policy.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To create a service-policy for outbound traffic on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 237/1/8
switch(conf-if-te-237/1/8)# service-policy out policymap1
```

To remove a service-policy for outbound traffic from a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 237/1/8
switch(conf-if-te-237/1/8)# no service-policy out
```

To remove a service-policy for inbound traffic on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 237/1/8
switch(conf-if-te-237/1/8)# no service-policy in
```

See Also **interface, class, qos cos, policy-map, show policymap**

set distance

Configures the route distance set clause in a route-map instance.

Synopsis **set distance** *value*

no set distance *value*

Operands

value	The distance clause for the route-map instance.

Defaults None

Command Modes Privileged EXEC mode

Description This command configures the route distance set clause in a route-map instance.

Usage Guidelines Use the **no set distance** *value* command to disable this feature.

Examples None

See Also **ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set ip next-hop, set metric, set tag**

set ip next-hop

Configures the route next-hop set clause in a route-map instance.

Synopsis **set ip next-hop** *A.B.C.D*

no set ip next-hop *A.B.C.D*

Operands **next-hop** *A.B.C.D* The IP address for the next hop.

Defaults None

Command Modes Privileged EXEC mode

Description This command configures the route next-hop set clause in a route-map instance.

Usage Guidelines Use the **no set ip next-hop** *A.B.C.D* command to disable this feature.

Examples None

See Also **ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set metric, set tag**

set metric

Configures the route metric set clause in a route-map instance.

Synopsis **set metric** [**add** | **assign** | **sub**] *value*

no set metric [**add** | **assign** | **sub**] *value*

Operands

add	Adds the value to the route.
assign	Assigns the value to the route.
sub	Subtracts the value from the route.
value	Metric clause value.

Defaults None

Command Modes Privileged EXEC mode

Description Configures the route metric set clause in a route-map instance. The add, assign, sub operators change the current route metric value by add to, replace, and subtract from it.

Usage Guidelines Use the **no set metric** command to disable this feature.

Examples None

See Also **ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set ip next-hop, set tag**

set tag

Configures the route tag set clause in a route-map instance.

Synopsis **set tag** *value*

no set tag *value*

Operands

value	The tag clause value for the route-map.

Defaults None

Command Modes Privileged EXEC mode

Description This command configures the route tag set clause in a route-map instance.

Usage Guidelines Use the **no set tag** *value* command to disable this feature.

Examples None

See Also **ip prefix-list**, **match interface**, **match ip address**, **match ip next-hop**, **match metric**, **match route-type**, **match tag**, **route-map**, **set distance**, **set ip next-hop**, **set metric**

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 None

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
```

See Also None

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.

On the Brocade VDX 8770, SPAN and sFlow can be enabled at the same time. On the Brocade VDX 6720, SPAN and sFlow cannot be enabled at the same time.

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 subconfiguration mode (fo, gi, te).

Description Use this command to enable sFlow on a specific interface. sFlow is used for monitoring network activity.

Usage Guidelines This command is supported on physical ports only.

On the Brocade VDX 8770, SPAN and sFlow can be enabled at the same time. On the Brocade VDX 6720, SPAN and sFlow cannot be enabled at the same time.

Use the **no sflow enable** command to disable sFlow on an interface.

Examples To enable sFlow on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# sflow enable
```

See Also **interface**, **sflow enable (global version)**, **sflow polling-interval (interface version)**, **sflow sample-rate (interface 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 None

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 subconfiguration mode (fo, gi, te).

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.

Usage Guidelines Use the **no sflow polling interval** command to return to the default value.

Examples To set the polling interval to 135 seconds on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# sflow polling-interval 135
```

See Also **interface**, **sflow polling-interval (global version)**, **sflow enable (interface version)**, **sflow sample-rate (interface 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 default sampling rate for an 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 16777215. The default value is 32768.

Defaults The default is the current global default sampling in packets.

Command Modes Interface subconfiguration mode (fo, gi, te).

Description Use this command to change the default sampling rate for a specific interface. This determines how many packets are skipped before the next sample is taken for that 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 on a specific fortygigabitethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# sflow sample-rate 4096
```

See Also **interface**, **sflow sample-rate (global version)**, **sflow enable (interface version)**, **sflow polling-interval (interface version)**

short-path-forwarding

Enables short-path forwarding on the virtual router.

Synopsis **short-path-forwarding**

no short-path-forwarding

Operands There are no operands for this command.

Default Disabled

Command Modes Virtual-router-group configuration mode.

Description Enables short-path forwarding on the virtual router. Short-path forwarding means that a backup physical router in a virtual router attempts to bypass the VRRP-E master router and directly forward packets through interfaces on the backup router.

Usage Guidelines This command can be used for VRRP-E, but for VRRP. You can perform this configuration on a ve interface only. Use the **no** parameter with this command to remove this configuration.

Examples To enable short-path-forwarding on a VRRP-E group:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-Ve-25)# vrrp-extended-group 100
switch(config-vrrp-extended-group-100)# short-path-forwarding
```

See Also **vrrp-group**

show access-list

Displays the status of all ACLs bound to a particular interface

Synopsis **show access-list** {**ip** | **mac**} *name* {**port-channel** *index* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **fortygigabitethernet** *slot/port* | vlan *vlanId* | ve *vlanId*} {**in** | **out**}

Operands

ip | *mac*	Displays the configured rules of either a L2 or L3 ACL.
name	The “name” of the ACL assigned at creation.
port-channel *index*	Specifies the port-channel index to which the ACL is bound.
gigabitethernet *slot/port*	Specifies the gigabitethernet interface to which the ACL is bound.
tengigabitethernet *slot/port*	Specifies the ten gigabitethernet interface to which the ACL is bound.
fortygigabitethernet *slot/port*	Specifies the forty gigabitethernet interface to which the ACL is bound.
vlan *vlanId*	Specifies the VLAN interface to which the ACL is bound.
ve *vlanId*	Specifies the Virtual Ethernet interface to which the ACL is bound.
in | **out**	Specifies the ACL binding direction (ingress or egress).

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the status of all ACLs bound to a particular interface.

Usage Guidelines None

Examples None

See Also None

show access-list interface

Displays the status of all ACLs bound to a particular interface

Synopsis **show access-list interface** {**port-channel** *index* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **fortygigabitethernet** *slot/port* | **vlan** *vlanId* | **ve** *vlanId*} {**in** | **out**}

Operands

port-channel *index* Specifies the port-channel index to which the ACL is bound.

gigabitethernet *slot/port*
Specifies the gigabitethernet interface to which the ACL is bound.

tengigabitethernet *slot/port*
Specifies the ten gigabitethernet interface to which the ACL is bound.

fortygigabitethernet *slot/port*
Specifies the forty gigabitethernet interface to which the ACL is bound.

vlan *vlanId* Specifies the VLAN interface to which the ACL is bound.

ve *vlanId* Specifies the Virtual Ethernet interface to which the ACL is bound.

in | **out** Specifies the ACL binding direction (ingress or egress).

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the status of all ACLs bound to a particular interface.

Usage Guidelines None

Examples None

See Also None

show arp

Displays the ARP cache.

Synopsis **show arp** [{**summary** | **dynamic** | **static** [**summary**]} | **ip** *ip-address* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies 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 None

Command Modes Privileged EXEC mode

Description Use this command to display the contents of the ARP cache.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples None

See Also None

show autoupload

Displays the autoupload configuration.

Synopsis **show autoupload** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for rbridge-id include the following:
rbridge-id	*Specifies the ID of the routing bridge. This option is not valid in standalone mode.*
all	Specifies all switches in the fabric.

Defaults Displays information for the local switch. The output displays the host configuration, upload protocol, and whether or not the autoupload feature is enabled.

Command Modes Privileged EXEC mode.

Description Use this command to display the autoupload configuration for the specified switches.

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

Examples To display the autoupload configuration on the local switch:

```
switch# show autoupload
Host IP Addr: 10.38.33.131
User name:admin
Remote Dir: /home/admin/support
Auto Upload protocol:   ftp
Auto-FTP:      On
```

See Also **clear support, copy support, show support**

show calendar

Displays the current date and time based on the switch hardware clock.

Synopsis **show calendar**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current date and time based on the switch hardware clock.

Usage Guidelines None

Examples To display calendar information:

```
switch# show calendar
16:33:30 UTC Tue Feb 14 2012
```

See Also None

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 onthe 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 v3.0.0 only allows the CEE map named “default.”

Examples None

See Also **cee, cee-map (configuration)**

show cert-util ldapca

Displays the LDAP CA certificate.

Synopsis **show cert-util ldapca**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display theLightweight Directory Access Protocol (LDAP) Certification Authority (CA) certificate.

Usage Guidelines None

Examples To display the LDAP certificate on the switch:

```
switch# show cert-util ldapca
LDAP CA
```

See Also **ldap-server host, ldap-server maprole, show running-config ldap-server, username**

show chassis

Displays all field-replaceable units (FRUs).

Synopsis **show chassis** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. Only the local RBridge ID is currently supported.
all	Specifies all switches in the fabric. This option is not supported.

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. Chassis family, for example VDX 8770.
2. The chassis backplane revision.
3. Object type: MM (management module), SFM (switch fabric module), LC (line card), CHASSIS, FAN, POWER SUPPLY, SW CID (chassis ID), WWN (world wide name), or UNKNOWN.
4. Object number: Slot number (for blades), Unit number (for everything else).
5. If the FRU is part of an assembly, a brief description displays in parentheses.
6. FRU header version number (Header Version: x) or blade version.
7. The object's maximum allowed power consumption: a positive value for power supplies and a negative value for consumers. Power Consume Factor: *-xxx*.
8. A real-time power usage value is displayed for each FRU that supports real-time power measurement. When the capability is not supported for a FRU, the line is suppressed. Power Usage is displayed in Watts:
9. Part number (up to 14 characters): Factory Part Num: *xx-xxxxxx-x x*
10. Serial number (up to 12 characters): Factory Serial Num: *xxxxxxxxxx*
11. FRU manufacture date: Manufacture: Day: *dd* Month: *mm* Year: *yyyy*
12. Date of the last FRU header update: Update: Day: *dd* Month: *mm* Year: yyyy
13. Cumulative time, in days, that the FRU has been inserted in the chassis with Network OS running: Time Alive :*dd* days
14. Current time, in days, since the FRU was last powered on or the system was restarted: Time Awake: *dd* days
15. Externally supplied ID (up to 10 characters): ID: *xxxxxxxxxx*
16. Externally supplied part number (up to 20 characters): Part Num: *xxxxxxxxxxxxxxxxxxx*
17. Externally supplied serial number (up to 20 characters): Serial Num: *xxxxxxxxxxxxxxxxxxx*
18. Externally supplied revision number (up to 4 characters): Revision Num: *xxxx*

Usage Guidelines 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

This command is supported only on the local switch.

Pagination is not supported with this command. Use the more option to display the output one page at a time.

Examples To display the FRU information on a Brocade VDX 6720-24:

```
switch# show chassis rbridge-id 9

switchType: 96

FAN  Unit: 1
Time Awake:             64 days

FAN  Unit: 2
Time Awake:             64 days

POWER SUPPLY  Unit: 1
Header Version:         2
Factory Part Num:       40-1000590-03
Factory Serial Num:     BWU0406G006
Manufacture:            Day: 18  Month:  2  Year: 2011
Update:                 Day:  1  Month:  7  Year: 2012
Time Alive:             594 days
Time Awake:             0 days

POWER SUPPLY  Unit: 2
Header Version:         2
Factory Part Num:       40-1000590-03
Factory Serial Num:     BWU0406G006
Manufacture:            Day: 18  Month:  2  Year: 2011
Update:                 Day:  1  Month:  7  Year: 2012
Time Alive:             594 days
Time Awake:             64 days

CHASSIS/WWN  Unit: 1
Header Version:         2
Power Consume Factor:   0
Factory Part Num:       40-1000590-03
Factory Serial Num:     BWU0406G006
Manufacture:            Day: 18  Month:  2  Year: 2011
Update:                 Day:  1  Month:  7  Year: 2012
Time Alive:             594 days
Time Awake:             64 days
```

To display the FRU information on a Brocade VDX 8770-4:

```
switch# show chassis rbridge-id 1

Chassis Family:         VDX87xx
Chassis Backplane Revision: 2

switchType: 1000

MM  Slot: M1
Blade Version:          3
Power Consume Factor:   -120
Power Usage (Watts):    -43
```

```
Factory Part Num:       60-1002179-07
Factory Serial Num:     BVT0329G00D
Manufacture:            Day: 26  Month:  7  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             78 days
Time Awake:             1 days

SFM  Slot: S2
Blade Version:          3
Power Consume Factor:   -150
Power Usage (Watts):    -132
Factory Part Num:       60-1002180-05
Factory Serial Num:     BVU0321G01F
Manufacture:            Day: 39  Month:  5  Year: 17
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             76 days
Time Awake:             1 days

LC  Slot: L1
Blade Version:          3
Power Consume Factor:   -400
Factory Part Num:       60-1002181-08
Factory Serial Num:     BVV0333G00E
Manufacture:            Day: 17  Month:  8  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             69 days
Time Awake:             1 days

LC  Slot: L2
Blade Version:          3
Power Consume Factor:   -400
Factory Part Num:       60-1002181-07
Factory Serial Num:     BVV0326G01B
Manufacture:            Day:  5  Month:  7  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             75 days
Time Awake:             1 days

LC  Slot: L3
Blade Version:          3
Power Consume Factor:   -400
Power Usage (Watts):    -261
Factory Part Num:       40-1000573-01
Factory Serial Num:     BTF0333G002
Manufacture:            Day: 48  Month:  8  Year: 17
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             58 days
Time Awake:             1 days

LC  Slot: L4
Blade Version:          3
Power Consume Factor:   -400
Factory Part Num:       60-1002181-07
Factory Serial Num:     BVV0326G01A
Manufacture:            Day:  5  Month:  7  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             80 days
Time Awake:             1 days

POWER SUPPLY  Unit: 1
```

```
Power Consume Factor:   3000
Factory Part Num:       23-0000135-01
Factory Serial Num:     BMM2J02G003
Manufacture:            Day:  1  Month:  1  Year: 2011
Time Awake:             1 days
ID:                     LPCS
Part Num:               SP750Z1A
Rework:                 A

POWER SUPPLY  Unit: 2
Power Consume Factor:   3000
Factory Part Num:       23-0000135-01
Factory Serial Num:     BMM2J02G008
Manufacture:            Day:  1  Month:  1  Year: 2011
Time Awake:             1 days
ID:                     LPCS
Part Num:               SP750Z1A
Rework:                 A

FAN  Unit: 1
Power Consume Factor:   -126
Power Usage (Watts):    -19
Factory Part Num:       60-1002130-02
Factory Serial Num:     BYX0320G007
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days

FAN  Unit: 2
Power Consume Factor:   -126
Power Usage (Watts):    -21
Factory Part Num:       60-1002130-02
Factory Serial Num:     BYX0320G011
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days

CID  Unit: 1
Power Consume Factor:   -1
Factory Part Num:       60-1002178-01
Factory Serial Num:     BWF0319G015
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days

CID  Unit: 2
Power Consume Factor:   -1
Factory Part Num:       60-1002178-01
Factory Serial Num:     BWF0319G01Z
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days

Chassis Factory Serial Num: BZA0320G00W
```

See Also show linecard, show mm, show sfm

show cipherset

Displays the current cipherset status.

Synopsis **show cipherset**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current cipherset status for LDAP and SSH.

Usage Guidelines None

Examples To display cipherset status on the switch:

```
switch# show cipherset
LDAP Cipher List        : !DH:HIGH:-MD5
SSH Cipher List         : 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
```

See Also **cipherset**

show clock

Returns the local time, date, and time zone.

Synopsis **show clock rbridge-id** [*rbridge-id* | **all**]

Operands **rbridge-id**

rbridge-id	Specifies the unique identifier for the switch on which the local time, date, and time zone displays.
all	For this release, specifying **all** returns only local information.

Defaults The local clock is used unless the Rbridge ID or all is specified.

Command Modes Privileged EXEC mode

Description Use this command to display the current local clock and time zone.

Usage Guidelines This command is currently supported only on the local RBridge.

Examples The following example displays the local time, date, and time on the local clock:

To show the local switch clock time

```
switch# show clock
rbridge-id 1: 2012-05-04 16:01:51 Etc/GMT+0
```

See Also **clock set, clock timezone, ntp server**

show copy-support status

Displays the status of the copy support operation.

Synopsis **show copy-support status [{rbridge-id** *rbridge-id* **| all}]**

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for rbridge-id include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode.
all	Specifies all switches in the fabric.

Defaults Displays local switch information.

Command Modes Privileged EXEC mode

Description Use this command to display the status of the copy support operation. The status is indicated by the percentage of completion. On a modular chassis, this command displays status information for each module along with the slot number and SS type. NORMAL indicates process is proceeding or completed without errors. FAULTY indicates a faulty blade.

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

Examples To display the support upload status on a Brocade VDX 8770-4:

```
switch# show copy-support status

Slot Name        SS type         Completion Percentage
#########################################################
M1               NORMAL          [100%]
M2               NORMAL          [100%]
L1/0             NORMAL          [100%]
L1/1             NORMAL          [100%]
L2/0             NORMAL          [100%]
L2/1             NORMAL          [100%]
L4/0             NORMAL          [100%]
L4/1             NORMAL          [100%]
```

See Also **copy support, copy support-interactive, show support**

show debug ip igmp

Displays the IGMP packets received and transmitted, as well as related events.

Synopsis **show debug ip igmp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the IGMP packets received and transmitted.

Usage Guidelines None

Examples None

See Also None

show debug lacp

Displays the configured debugging features for LACP.

Synopsis **show debugging lacp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the configured debugging features for LACP.

Usage Guidelines None

Examples None

See Also None

show debug lldp

Displays the LLDP debugging status on the switch.

Synopsis **show debug lldp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the LLDP debugging status on the switch.

Usage Guidelines None

Examples To display the LLDP debugging status on the switch:

```
switch# show debug lldp
LLDP debugging status:
Interface te0/0    : Transmit Receive  Detail
```

See Also None

show debug spanning-tree

Displays the STP debugging status on the switch.

Synopsis **show debug spanning-tree**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the STP debugging status on the switch.

Usage Guidelines This command is available only in standalone mode.

Examples None

See Also None

show debug vrrp

Displays debug option(s).

Synopsis **show debug vrrp**

Operands There are no operands for this command.

Default None

Command Modes Privileged EXEC mode.

Description Displays the currently set debug option(s).

Usage Guidelines This command is for VRRP and VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples If you run this command and the debug option has already been set to debug all VRRP events, the following is displayed:

```
switch# show debug vrrp
   VRRP event debugging is on
```

show default-vlan

Displays the current default VLAN value.

Synopsis **show default-vlan**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current default VLAN value.

Usage Guidelines None

Examples None

See Also **reserved-vlan, show running reserved-vlan**

show diag burninerrshow

Displays the error messages that are stored in the nonvolatile storage on the slot during the POST and system verification processes.

Synopsis **show diag burninerrshow** [*rbridge-id*]

Operands

rbridge-id	Specifies the Rbridge ID of the switch for which errors stored in the storage on the slot during POST and system verification are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display errors that are stored in nonvolatile storage on the slot during POST and system verification.

Usage Guidelines None

Examples The error messages are updated when there is a POST failure or a systemVerification failure. To display burn-in errors from the switch:

```
switch# show diag burninerrshow rbridge-id 1

errLog for slot M2
errLog is empty for slot M2
errLog for slot S1
errLog is empty for slot S1
errLog for slot S2
errLog is empty for slot S2
errLog for slot S3
errLog is empty for slot S3
errLog for slot L4
errLog is empty for slot L4
rbridgeId 1
```

See Also **diag burninerrclear, diag clearerror, show diag burninstatus**

show diag burninerrshowerrLog

Displays the error log messages that are stored in the nonvolatile storage on the slot during the POST and system verification processes.

Synopsis **show diag burninerrshowerrLog**

Operands **slot** *slot_id* Specifies the slot ID. This is mandatory for slot-based systems only.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display error log messages that are stored in nonvolatile storage on the slot during POST and system verification.

Usage Guidelines None

Examples The error messages are updated when there is a POST failure or a systemVerification failure. To display the error log messages on the slot:

```
switch# show diag burninerrshowerrLog
Log for slot M1errLog is empty for slot M1errLog for slot
S12012/06/03-07:11:17:038992, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4
" S1 verify: Starting run Sun Jun 3 07:11:14 PDT 2012 "Err# 0140045
0300:101:000:001:0:20: , OID:0x430c0000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:31:02:766063, [DIAG-5004], 0, M1, INFO,
chassis, DIAG-MANUAL4 " S1 verify: TESTED stat PASSED 5 cmds in 1 runs Therm
10 Vib 2 in 0 hr 18 min 53 sec (0:18:53)"Err# 0140045 0300:101:000:001:0:20: ,
OID:0x430c0000, iobuf.c, lineerrLog for slot S22012/06/03-07:11:16:618653,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S2 verify: Starting run Sun
Jun 3 07:11:13 PDT 2012 "Err# 0140045 0400:101:000:001:0:20: ,
OID:0x43100000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:30:39:636631, [DIAG-5004], 0, M1, INFO,
chassis, DIAG-MANUAL4 " S2 verify: TESTED stat PASSED 5 cmds in 1 runs Therm
10 Vib 2 in 0 hr 18 min 58 sec (0:18:58)"Err# 0140045 0400:101:000:001:0:20: ,
OID:0x43100000, iobuf.c, lineerrLog for slot S32012/06/03-07:11:12:838561,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S3 verify: Starting run Sun
Jun 3 07:11:09 PDT 2012 "Err# 0140045 0500:101:000:001:0:20: ,
OID:0x43140000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:30:35:017964, [DIAG-5004], 0, M1, INFO,
chassis, DIAG-MANUAL4 " S3 verify: TESTED stat PASSED 5 cmds in 1 runs Therm
10 Vib 2 in 0 hr 19 min 4 sec (0:19:4)"Err# 0140045 0500:101:000:001:0:20: ,
OID:0x43140000, iobuf.c, line:errLog for slot L12012/06/03-07:11:18:678484,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L1 verify: Starting run Sun
Jun 3 07:11:15 PDT 2012 "Err# 0140045 0700:101:000:001:0:20: ,
OID:0x431c0000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:30:56:177298, [DIAG-5004], 0, M1, INFO,
chassis, DIAG-MANUAL4 " L1 verify: TESTED stat PASSED 8 cmds in 1 runs Therm
10 Vib 2 in 0 hr 18 min 44 sec (0:18:44)"Err# 0140045 0700:101:000:001:0:20: ,
OID:0x431c0000, iobuf.c, lineerrLog for slot L22012/06/03-07:11:18:678576,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L2 verify: Starting run Sun
Jun 3 07:11:15 PDT 2012 "Err# 0140045 0800:101:000:001:0:20: ,
OID:0x43200000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:30:40:774116, [DIAG-5004], 0, M1, INFO,
chassis, DIAG-MANUAL4 " L2 verify: TESTED stat PASSED 8 cmds in 1 runs Therm
10 Vib 2 in 0 hr 18 min 41 sec (0:18:41)"Err# 0140045 0800:101:000:001:0:20: ,
```

```
OID:0x43200000, iobuf.c, lineerrLog for slot L32012/06/03-07:11:17:097345,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L3 verify: Starting run Sun
Jun 3 07:11:14 PDT 2012 "Err# 0140045 0900:101:000:001:0:20: ,
OID:0x43240000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:19:29:651740, [DIAG-5046], 0, M1, ERROR,
chassis, L3:portLoopbackTest FAILED. Err -2, OID:0x43240000, diag_mercury_mm,
line: 543, comp:diag,
ltime:2012/06/03-07:19:29:6516992012/06/03-07:29:52:276612, [DIAG-5004], 0,
M1, INFO, chassis, DIAG-MANUAL4 " L3 verify: TESTED stat FAILED 8 cmds in 1
runs Therm 10 Vib 2 in 0 hr 18 min 34 sec (0:18:34)"Err# 0140045
0900:101:000:001:0:20: , OID:0x43240000, iobuf.c, lineerrLog for slot
L42012/06/03-07:11:17:385343, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4
" L4 verify: Starting run Sun Jun 3 07:11:15 PDT 2012 "Err# 0140045
0A00:101:000:001:0:20: , OID:0x43280000, iobuf.c, line: 648, comp:insmod,
ltime:2012/06/03-07:2012/06/03-07:30:27:647391, [DIAG-5004], 0, M1, INFO,
chassis, DIAG-MANUAL4 " L4 verify: TESTED stat PASSED 8 cmds in 1 runs Therm
10 Vib 2 in 0 hr 18 min 55 sec (0:18:55)"Err# 0140045 0A00:101:000:001:0:20: ,
OID:0x43280000, iobuf.c, linerbridgeId 233M4_237_233#
```

See Also **diag burninerrclear, diag clearerror, show diag burninstatus**

show diag burninstatus

Displays the diagnostics burn-in status or system verification status stored in the non-volatile storage memory in the switch.

Synopsis **show diag burninstatus** [*rbridge-id*]

Operands *rbridge-id* Specifies the Rbridge ID for the switch you want diagnostics burn-in status.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the burn-in status for a switch.

Usage Guidelines None

Examples To display the diagnostics burn-in status:

```
switch# show diag burninstatus
DiagID  State           Status  Run     Cmd     TotCmds PID
Script  SlotID
1       COMPLETE_TESTED PASS    1       8       8       23163   verify  L1
2       COMPLETE_TESTED PASS    1       8       8       23311   verify  L2
6       COMPLETE_TESTED PASS    1       5       5       23465   verify  S2
7       COMPLETE_TESTED PASS    1       5       5       23618   verify  S3
8       COMPLETE_TESTED PASS    1       5       5       23787   verify  S4
9       COMPLETE_TESTED PASS    1       5       5       23976   verify  S5
10      COMPLETE_TESTED PASS    1       5       5       24156   verify  S6
12      COMPLETE_TESTED PASS    1       8       8       24388   verify  L6
14      COMPLETE_TESTED PASS    1       8       8       24692   verify  L8
rbridgeId 1
```

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 on the switch.

Synopsis **show diag post results** {**brief** | **detailed**} [*rbridge-id*]

Operands

brief | detailed	Specifies whether the POST passed or failed (brief) or displays detailed status with the register dump when a POST fails (detailed).
rbridge-id	Specifies the Rbridge ID of the switch on which the diagnostic POST results are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display either the brief results or details of the last diagnostic POST that was executed.

Usage Guidelines None

Examples To display brief POST results (whether the POST passed or failed):

```
switch# show diag post results brief slot L4
POST1:Slot L4 turboramtest PASSED (exit_status 0).
POST1:Slot L4 Script PASSED with exit_status of 0 Thu Jan 1 00:04:36 GMT 1970
took (0:0:47)
POST2:Slot L4 portloopbacktest PASSED (exit_status 0).
POST2:Slot L4 prbstest PASSED (exit_status 0).
POST2:Slot L4 Script PASSED with exit_status of 0 Thu Jan 1 00:05:52 GMT 1970
took (0:1:15)
rbridgeId 1

switch# show diag post results detailed slot S1
POST1:Slot S1 Started running Thu Jan 1 00:02:46 GMT 1970
POST1:Slot S1 Running diagclearerror
POST1:Slot S1 Running diagsetup
POST1:Slot S1 Test #1 - Running turboramtest
Running turboramtest...
:
<..cut..>
:
POST1:Slot S1 ********** Slot S1 POST Summary **********
POST1:Slot S1 Completed 1 Diagnostic test:
POST1:Slot S1 Script PASSED with exit_status of 0 Thu Jan 1 00:02:53 GMT 1970
took (0:0:7)
POST2:Slot S1 Started running Thu Jan 1 00:02:58 GMT 1970
POST2:Slot S1 Running diagclearerror
POST2:Slot S1 Test #1 - Running portloopbacktest
Running portloopbacktest...
:
<..cut..>
:
POST2: ********** Slot S1 POST Summary **********
POST2:Slot S1 Completed 2 Diagnostic test:
```

```
POST2:Slot S1 Script PASSED with exit_status of 0 Thu Jan 1 00:03:35 GMT 1970
took (0:0:37)
rbridgeId 1
```

See Also **diag post enable**

show diag setcycle

Displays the current systemVerification test parameters.

Synopsis **show diag setcycle** [*rbridge-id*]

Operands

rbridge-id	Specifies Rbridge ID of the switch on which current values are displayed in system verification.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display current values used in system verification.

Usage Guidelines None

Examples To display current values used in system verification:

```
switch# show diag setcycle

CURRENT - KEYWORD           : DEFAULT
 1      - number_of_runs    :  1
 2      - min_lb_mode       :  2
 1      - tbr_passes        :  1
 16     - plb_nframes       : 16
 1      - pled_passes       :  1
rbridgeId 1
```

See Also **diag setcycle**

show diag status

Displays the currently diagnostic test status on one or all slots in the system.

Synopsis **show diag status** [*rbridge-id*]

Operands

rbridge-id	Specifies the Rbridge ID of the switch to display. If not specified, diagnostic tests for all blades in the system are displayed.
slot *slot_id*	Specifies the slot ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display currently running diagnostic tests on a specified switch.

Usage Guidelines None

Examples To automatically display current diagnostic status in the console:

```
switch# show diag status rbridge-id 1

Slot M2 [2]: DIAG runs 'NONE'
Slot S1 [3]: DIAG runs 'NONE'
Slot S2 [4]: DIAG runs 'NONE'
Slot S3 [5]: DIAG runs 'NONE'
Slot L4 [10]: DIAG runs 'NONE'
rbridgeId 1
```

To display the diagnostic status when POST is running on the LC or SFM using the slot ID:

```
switch# show diag status rbridge-id 233 slot L1

Slot L1 [7]:DIAG runs ‘turboramtest’
rbridgeId 233

switch# show diag status slot L1
Slot L1 [7]: DIAG runs ‘turboramtest’
rbridgeID 233
```

See Also **show diag post results**

show dot1x

Displays the overall state of dot1x on the system.

Synopsis **show dot1x**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the overall state of dot1x on the system.

Usage Guidelines None

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:         2
Auth Server:              RADIUS

RADIUS Configuration
--------------------
Position:                 1
Server Address:           172.21.162.51
Port:                     1812
Secret:                   sharedsecret
Position:                 2
Server Address:           10.32.154.113
Port:                     1812
Secret:                   sharedsecret
```

See Also None

show dot1x all

Displays detailed dot1x information for all of the ports.

Synopsis **show dot1x all**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display detailed information for all of the ports.

Usage Guidelines None

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:         2
Auth Server:              RADIUS

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
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 Address:       0000.0000.0000
Current Id:               1
Id From Server:           0
```

See Also None

show dot1x diagnostics interface

Displays all diagnostics information for the authenticator associated with a port.

Synopsis **show dot1x diagnostics interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display all diagnostics information for the authenticator associated with a port.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display all diagnostics information for the authenticator associated with a port:

```
switch# show dot1x diagnostics interface tengigabitethernet 5/0/16
802.1X Diagnostics for interface te5/0/16
 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
```

See Also None

show dot1x interface

Displays the state of a specified interface.

Synopsis **show dot1x interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the state of a specified interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display the state of 10 Gbps Ethernet interface 0/16:

```
switch# show dot1x interface tengigabitethernet 5/0/16
Dot1x Global Status:      Enabled
802.1X info for interface te5/0/16
---------------------------------
Port Control:             Auto
Port Auth Status:         Unauthorized
Protocol Version:         2
ReAuthentication:         Disabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
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 Address:       0000.0000.0000
Current Id:               1
Id From Server:           0
```

See Also None

show dot1x session-info interface

Displays all statistical information of an established session.

Synopsis **show dot1x session-info interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display all statistical information of the established session for a specified interface.

Usage Guidelines None

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
```

See Also None

show dot1x statistics interface

Displays the statistics of a specified interface.

Synopsis **show dot1x statistics interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the statistics of a specified interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display the statistics for 10 Gbps Ethernet interface 22/0/16:

```
switch# show dot1x statistics interface tengigabitethernet 22/0/16
802.1X statistics for interface te22/0/16
  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
```

See Also None

show dpod

Displays Dynamic Ports on Demand (POD) license information.

Synopsis **show dpod** [*rbridge-id* | **all**]

Operands

rbridge-id	Executes the command on the remote switch specified by the RBridge ID.
all	Executes the command on all switches in the cluster.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display Dynamic POD license information for the local switch.

Usage Guidelines The Dynamic POD feature is not supported on the Brocade VDX 6710 or VDX 8770.

In the Network OS v3.0.0 release this command displays only on the local RBridge.

Examples To display Dynamic POD assignment information:

```
switch# show dpod
rbridge-id: 1
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 1/0/1, Te 1/0/10, Te 1/0/11, Te 1/0/12, Te 1/0/13, Te 1/0/14, Te
1/0/15, Te 1/0/16, Te 1/0/17, Te 1/0/18, Te 1/0/19, Te 1/0/20, Te 1/0/21, Te
1/0/22, Te 1/0/23, Te 1/0/24
  Ports assigned to the first POD license:
     Te 1/0/5, Te 1/0/6, Te 1/0/7, Te 1/0/8, Te 1/0/9
  Ports assigned to the second POD license:
     None
  Ports not assigned to a license:
     Te 1/0/2, Te 1/0/3, Te 1/0/4

    3 license reservations are still available for use by unassigned ports
```

See Also dpod, **show running-config dpod**

show edge-loop-detection globals

Displays ELD global configuration values.

Synopsis **show edge-loop-detection globals**

Operands None

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to view the configured values for PDU receive limit, shutdown time, and hello time.

Usage Guidelines This functionality detects Layer 2 loops only.

Examples To view the ELD global configuration values:

```
switch# show edge-loop-detection globals


Edge-loop-detection global configuration values are as below:

PDU receive limit (packets):    1
Shutdown-time (minutes):        0
Hello-time (msec):              1000
```

See Also edge-loop-detection VLAN, hello-interval, pdu-rx-limit, protocol edge-loop-detection, shutdown-time

show edge-loop-detection interface

Displays ELD interface configuration information and packet statistics.

Synopsis **show edge-loop-detection interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel number**}

Operands

tengigabitethernet	**Specifies a valid 10 Gbps Ethernet interface.**
rbridge-id	Specifies the ID of the routing bridge. This value is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This value is not valid in standalone mode.
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 6144 for Brocade VCS Fabric mode.

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to view the ELD configuration settings and status for a specific interface and to view the number of packets received and transmitted.

Usage Guidelines None

Examples To view the ELD status for a specific interface:

```
switch(conf-if-te-7/0/5)# do show edge-loop-detection interface
tengigabitethernet 7/0/5
Number of eld instances: 1
Enabled on VLANs:       100
Priority:               128
Interface status:       UP
Auto enable in:         Never

Packet Statistics:
vlan            sent            rcvd
100             100               0
```

See Also clear edge-loop-detection, edge-loop-detection VLAN, edge-loop-detection port-priority, protocol edge-loop-detection, shutdown-time

show edge-loop-detection rbridge-id

Displays ELD status information for a specific routing bridge.

Synopsis **show edge-loop-detection rbridge-id** *rbridge-id*

Operands *rbridge-id* Specifies the ID of the routing bridge.

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to view the configuration and status of ELD on a specific routing bridge, including the ports that ELD has disabled. For each interface on which ELD is enabled, this command shows the enabled VLANs, the ELD port priority, the up/down status of the interface, and time to the next automatic port re-enable.

Usage Guidelines This functionality detects Layer 2 loops only.

Examples To view the ELD status:

```
switch# show edge-loop-detection rbridge-id 7
Number of edge-loop-detection instances enabled: 1

Interface: 7/0/5
------------------------
        Enabled on VLANs: 100
        Priority:       128
        Interface status: UP
        Auto enable in: Never
```

See Also clear edge-loop-detection, edge-loop-detection VLAN, edge-loop-detection port-priority, shutdown-time

show environment fan

Displays fan status information.

Synopsis **show environment fan** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

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 maximum	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. This value is not applicable to modular chassis.
speed	Fan RPM.

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

Pagination is not supported with this command. Use the more option to display the output one page at a time.

Examples To display the fan status information on a Brocade VDX 6720-24:

```
switch# show environment fan

Fan 1 is Ok, speed is 2057 RPM
Fan 2 is Ok, speed is 2009 RPM
Airflow direction : Port side exhaust
```

To display the fan status information on a Brocade VDX 8770-4:

```
switch# show environment fan

Fan 1 is Ok, speed is 2057 RPM
Fan 2 is Ok, speed is 2009 RPM
```

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** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

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) or chassis ID (CID) 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 modular platforms: CHASSIS, CID (chassis ID card), FAN, POWER SUPPLY, SW BLADE (port blade), MM[1-2] (management module) ,SFM (switch fabric module),LC[1-8] (line 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 FRU serial number (xxxxxxxxxxx) or Not available.

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

Pagination is not supported with this command. Use the more option to display the output one page at a time.

Examples To display the FRU history on a Brocade VDX 6720-24:

```
switch# show environment history

FAN  Unit 1             Inserted at Wed Mar 30 19:19:55 2011
Factory Part Number:    Not Available
Factory Serial Number:  Not Available

FAN  Unit 2             Inserted at Wed Mar 30 19:19:56 2011
Factory Part Number:    Not Available
Factory Serial Number:  Not Available
```

```
POWER SUPPLY  Unit 1    Inserted at Wed Mar 30 19:19:56 2011
Factory Part Number:    Not Available
Factory Serial Number:  Not Available

POWER SUPPLY  Unit 2    Inserted at Wed Mar 30 19:19:56 2011
Factory Part Number:    Not Available
Factory Serial Number:  Not Available

Records:  4
```

To display the FRU history on a Brocade VDX 8770-4

```
switch# show environment history

CID  Unit 2             Inserted at Tue Sep  6 22:40:27 2011
Factory Part Number:    40-1000592-01
Factory Serial Number:  BVW0311G00K

SFM  Slot 3             Inserted at Tue Sep  6 22:41:47 2011
Factory Part Number:    60-1002180-05
Factory Serial Number:  BVU0321G00N

LC  Slot 9              Inserted at Tue Sep  6 22:41:48 2011
Factory Part Number:    60-1002181-07
Factory Serial Number:  BVV0326G019

LC  Slot 10             Inserted at Tue Sep  6 22:41:50 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G01F

MM  Slot 1              Inserted at Tue Sep  6 22:41:50 2011
Factory Part Number:    60-1002179-07
Factory Serial Number:  BVT0329G00B

SFM  Slot 4             Inserted at Wed Sep  7 00:01:44 2011
Factory Part Number:    60-1002180-06
Factory Serial Number:  BVU0329G00B

LC  Slot 10             Removed at Mon Sep 12 19:04:58 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G01F

LC  Slot 10             Inserted at Mon Sep 12 19:12:21 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G01F

LC  Slot 1              Inserted at Mon Sep 12 19:19:52 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G00B
(output truncated)
```

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** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the type and current status of the switch power supply. The status of the power supply 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. Replace the power supply as soon as possible.
faulty	Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).
Airflow	Direction of fan air flow (not applicable to modular chassis).

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

Examples To display the power supply status:

```
switch# show environment power

Power Supply #1 is OK
LPCS      F@ 11/01/18 type: AC V165.2 3000W
Power Supply #2 is OK
LPCS      F@ 11/01/18 type: AC V165.2 3000W
Power Supply #3 is absent
Power Supply #4 is absent
Power Supply #1 is faulty
```

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** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

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. Refer to the **show environment power** command for an explanation of the power supply status values.

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

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** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

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 sensor ID, the slot number (on modular chassis only), the sensor state, and the temperature. The temperature readings are given in both Centigrade and Fahrenheit.

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

Refer to the hardware reference manual for your switch to determine the normal temperature range.

Examples To display the temperature readings on a Brocade VDX 6720-24:

```
switch# show environment 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 Brocade VCS Fabric membership information.

Synopsis **show fabric all**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the fabric. If the switch is initializing or is disabled, the message “Local Switch disabled or fabric is re-building” is displayed. If the fabric is re-configuring, some or all switches may not be displayed; otherwise, the following fields are displayed:

VCS Id	VCS id of the switch
Config Mode	VCS mode of the switch. For fabric cluster mode, "Local-Only" is displayed.
Rbridge-id	The Rbridge-id of the switch.
WWN	The switch World Wide Name.
IP Address	The switch Ethernet IP address.
Name	The switch symbolic name. An arrow (>) indicates the principal switch. An asterisk (*) indicates the switch on which the command is entered.

Usage Guidelines The **show vcs** command returns the state as “disabled” if the switch is in standalone mode.This command can not be issued in Standalone mode.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

This command does not function in standalone mode.

Examples

```
switch# show fabric all
Config Mode: Local-Only
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"
The Fabric has 9 Rbridge(s)
```

The angle bracket (>), as shown with RBridge-ID 12-a, indicates the principal switch. The asterisk (*) indicates the switch on which the command was entered.

See Also **show vcs**

show fabric ecmp load-balance

Displays the current configuration of hash field selection and hash swap.

Synopsis **show fabric ecmp load-balance** [**rbridge-id** *value*]

Operands **rbridge-id** *value* Designates the RBridgeID for display?

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the current configuration of hash field selection and hash swap.

Usage Guidelines The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples Example output of command:

```
switch# show fabric ecmp load-balance
Fabric Ecmp Load Balance Information
------------------------------------
Rbridge-Id                  : 2
Ecmp-Load-Balance Flavor    : Destination MAC address and VID based load
balancing
Ecmp-Load-Balance HashSwap  : 0x4

switch# show fabric ecmp load-balance rbridge-id 2
Fabric Ecmp Load Balance Information
------------------------------------
Rbridge-Id                  : 2
Ecmp-Load-Balance Flavor    : Destination MAC address and VID based load
balancing
Ecmp-Load-Balance HashSwap  : 0x4
```

See Also **show fabric isl, show fabric trunk**

show fabric isl

Displays inter-switch link (ISL) information in the fabric.

Synopsis **show fabric isl** [*rbridge-id* | **all**]

Operands

rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
all	Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display ISL information in the fabric. If the ISL is segmented then "(segmented - incompatible)" displays in the output.

The command output includes the following information:

Rbridge-id	Rbridge-id of the switch. The range of valid values is from 1 through 239.
#ISLs	Number of ISLs connected.
Src Index	Source index of the local Rbridge.
Src Interface	Source interface of the local rbridge in the format “local-rbridge-id/slot/port”. If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	Neighbor Index of the ISL connected from local port. If the link is segmented and the NBR rbridge details are unavailable, "?" displays in this field.
Nbr Interface	Neighbor interface of the ISL connected from the local rbridge in the format “nbr-rbridge-id/slot/port”. If the ISL is not completely up, this field will be displayed as "?/?/?".
Nbr-WWN	Neighbor WWN of the switch. If the ISL is segmented and the neighbor rbridge details are not available, then "??:??:??:??:??:??:??:??" displays in this field.
BW	Bandwidth of the traffic.
Trunk	Displays "Yes" if trunk is enabled in the ISL.
Nbr-Name	Neighbor switch name.

Usage Guidelines This command is not available in standalone mode.

If this command is executed without operands, it displays the ISL information of local routing bridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

For segmented links, “(segmented - incompatible)” is displayed to indicate that the ISL is segmented. The Nbr Index, Nbr Interface, and Nbr-WWN files show question marks if the information is not known.

Examples The following example displays inter-switch link (ISL) information in the fabric.

```
switch# show fabric isl
Rbridge-id: 76   #ISLs: 2
Src       Src         Nbr       Nbr
 Index   Interface     Index   Interface             Nbr-WWN           BW   Trunk  Nbr-Name
-----------------------------------------------------------------------------------------------
 2     Te 1/0/2        56     Te 21/0/56     10:00:00:05:33:13:5F:BE  60G   Yes   "Edget12r1_1_21"
 7     Te 1/0/7        55     Te 22/0/55     10:00:00:05:33:40:31:93  40G   Yes   "Edget12r12_22"
```

The following example displays ISL information and includes a segmented link.

```
switch# show fabric isl
Rbridge-id: 2   #ISLs: 4
Src       Src        Nbr        Nbr
Index   Interface    Index    Interface         Nbr-WWN              BW   Trunk   Nbr-Name
-----------------------------------------------------------------------------------------
1       Te 2/0/1      1       Te 3/0/1      10:00:00:05:1E:CD:7A:7A  10G   Yes    "sw0"
2       Te 2/0/2      ?       Te ?/?/?      ??:??:??:??:??:??:??:?? (segmented - incompatible)
26      Te 2/0/26     56      Te 25/0/56    10:00:00:05:33:40:2F:C9  60G   Yes    "Edget12r31_25"
34      Te 2/0/34     58      Te 26/0/58    10:00:00:05:33:41:1E:B7  40G   Yes    "Edget12r32_26"
```

The following example displays ISL information and includes an Fi port.

```
switch# show fabric isl
Rbridge-id: 66   #ISLs: 5
 Src         Src         Nbr       Nbr
Index     Interface     Index   Interface      Nbr-WWN                   BW   Trunk  Nbr-Name
-----------------------------------------------------------------------------------------
  5       Te 66/0/5      1       Te 65/0/1     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
 15       Te 66/0/15     2       Te 65/0/2     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
 25       Te 66/0/25     3       Te 65/0/3     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
 35       Te 66/0/35     4       Te 65/0/4     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
124       Fi 66/0/4      7       Fi 2/-/-      50:00:51:E4:44:40:0E:04   32G   Yes   "fcr_fd_2"
```

See Also fabric isl enable, show diag burninstatus, show fabric isl, show fabric trunk

show fabric islports

Displays information for all inter-switch link (ISL) ports in the switch.

Synopsis **show fabric islports** [*rbridge-id*]

Operands

rbridge-id	Specifies the ID of the routing bridge on which the ISL ports are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information for all ISL ports in the switch. The command output includes the following information:

Name	Switch name.
Type	Switch model and revision number.
State	Switch state. The valid values are Online, Offline, Testing, or Faulty.
Role	Switch role. The valid values are Principal, Subordinate, or Disabled.
VCS Id	The range of valid values is from 1 through 8192
Config Mode	Brocade VCS Fabric mode. The valid values are Standalone/Local-Only/Distributed.
Rbridge-id	Rbridge-id of the switch. The range of valid values is from 1 through 239.
WWN	Switch world wide name (WWN).
FCF MAC	Mac address
Index	Port Index is a number between 0 and the maximum number of supported ports on the platform. The port index identifies the port number relative to the switch.
Interface	Interface of the local rbridge in the format "local-rbridge-id/slot/port".
State	Port state information:
Up	If the ISL is connected and the link is up
Down	No ISL is connected
Operational State	ISL state information:
ISL	Fabric port; displays the world wide name (WWN) and name of the attached switch.
(Trunk Primary)	The port is the master port in a group of trunking ports.
(Trunk port, primary is rbridge-id/slot/port)	The port is configured as a trunking port; the primary port is rbridge-id/slot/port.
(upstream)	The ISL is an upstream path toward the principal switch of the fabric.
(downstream)	The ISL is a downstream path away from the principal switch of the fabric.

Segmented, (Reason Code)
The ISL has been segmented due to the given reason code.

Down, (Reason Code)
The ISL is down due to the given reason code.

In this command, ISL segmentation is denoted as "ISL segmented, (segmentation reason)". The segmentation reason could be any one from Table 5.

TABLE 5 Segmentation reasons

Number	Segmentation	Explanation
1	RBridge-ID Overlap	When a new node joins the cluster with the RBridge-id already existing in the cluster.
2	ESC mismatch, Unknown	Only on one side of the ISL, the actual ESC mismatch reason code will be displayed. On the other end, Unknown will be displayed.
3	ESC mismatch, Config Mode	Brocade VCS Fabric mode is different on both switches.
4	ESC mismatch, Distributed Config DB	The DCM Configuration DB is different on both the ends of ISL.
5	ESC mismatch, Brocade VCS Fabric License	Brocade VCS Fabric license is enabled on one end and disabled on the other side.
6	ESC mismatch, Fabric Distribution Service	FDS state is different on both the ends.
7	zone conflict	Zone configuration is not same on both the switches.
8	ISL Disabled	This port is disabled to be an ISL.
9	ISL Isolated	If BF or DIA is rejected then the port will get isolated.
10	LD incompat	ECP rejected or retries exceeded.
11	FDS Zone Conflict	FDS configuration caused zone conflict.

In this command, disabled ports are denoted as "Down (Disabled reason)". The disabled reason could be any one from Table 6.

TABLE 6 Disabled port reasons

Number	Disabled Reasons	Explanation
1	Admin	Port is persistently disabled.
2	Protocol Incomplete	The ISL couldn't complete the link protocol. Stuck in G_PORT state.
3	RBridge-ID Overlap	Two nodes in the cluster requested for same Rbridge ID.
4	Long distance incompatability	Long distance configuration doesn't match.
5	ELP retries exceeded	Max ELP retires exceeded but no response from the other end.
6	Zone conflict	Zoning configuration overlaps.
7	ESC Config Mode Conflict	The link has been segmented due to different Brocade VCS Fabric mode.
8	ESC NOS incompatible	Other end doesn't support Brocade VCS Fabric technology.
9	ESC Distributed Config DB Conflict	DCM Configuration DB conflict.
10	ESC VCS Fabric License Conflict	Brocade VCS Fabric license is not enabled on one end.

TABLE 6 Disabled port reasons (Continued)

Number	Disabled Reasons	Explanation
11	No VCS Fabric License	Brocade VCS Fabric license is not enabled. For more than 2 nodes in the cluster VCS fabric license is mandatory.
12	ESC Fabric Distribution Service Conflict	FDS state is different.
13	Zoning FDS Configuration Conflict	FDS zoning configuration is different.

Usage Guidelines This command is not available in Standalone mode. If this command is executed without operands, it displays the ISL information of the local rbridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples To display information for all ISL ports in the core switch:

```
switch# show fabric islports
Name:    sw0
Type:    107.4
State:    Online
Role:    Fabric Subordinate
VCS Id:     10
Config Mode:Local-Only
Rbridge-id: 11
WWN:    10:00:00:05:33:6d:7f:77
FCF MAC:    00:05:33:6d:7f:77

 Index InterfaceState   Operational State
==========================================================================
  1 Te 11/0/1         Up  ISL 10:00:00:05:33:00:77:80 "sw0" (upstream)(Trunk Primary)
  2 Te 11/0/2         Down
  3 Te 11/0/3         Down
  4 Te 11/0/4         Up  ISL (Trunk port, Primary is Te 11/0/1 )
  5 Te 11/0/5         Down
  6 Te 11/0/6         Down
  7 Te 11/0/7         Down
  8 Te 11/0/8         Down
  9 Te 11/0/9         Down
 10 Te 11/0/10        Down
 11 Te 11/0/11        Up  ISL 10:00:00:05:1e:00:50:00 "sw0" (Trunk Primary)
121 Fi 11/0/1         Up  LS ISL 50:00:53:37:b6:93:5e:02 "fcr_fd_160" (downstream)(Trunk Primary)
122 Fi 11/0/2         Up  LS ISL (Trunk port, Primary is Fi 11/0/1 )
123 Fi 11/0/3         Down
124 Fi 11/0/4         Down
125 Fi 11/0/5         Down
```

See Also fabric isl enable, show diag burninstatus, show fabric isl, show fabric trunk

show fabric route linkinfo

Displays the Rbridge route link information connected in the fabric.

Synopsis **show fabric route linkinfo**

Operands **None**

Defaults None

Command Modes Privileged EXEC mode

Description This command displays details about all the links connected to the fabric. It groups the information for each routing bridge in the fabric.

The command displays the following fields of information:

Rbridge-id	ID of the routing bridge. The range of valid values is from 1 through 239.
Reachable	Indicates whether the routing bridge can be reached. Displays "Yes" if it is reachable, otherwise displays "No".
Version	Displays the version.
No. of links	The number of ISLs connected to the neighbor switches..
Link #	A sequence number for links on the routing bridge.
Src Index	E_Port interface on the local switch. This value is typically equal to the Index field reported in the **switchShow** command.
Src Interface	Source interface of the local rbridge in the format “local-rbridge-id/slot/port”. If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	E_Port interface on the remote switch. This value is typically equal to the index field reported in the **switchShow** command. If the link is segmented and the NBR rbridge details are unavailable, "?" displays in this field.
Nbr Interface	Neighbor interface of the ISL connected from the local rbridge in the format “nbr-rbridge-id/slot/port”. If the ISL is not completely up, this field will be displayed as "?/?/?".
Link-Cost	The cost of reaching the destination domain.
Link-type	The type of link.
Trunk	Displays "Yes" if trunk is enabled in the ISL, otherwise displays "No".

Usage Guidelines The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples To display link information for the fabric:

```
switch# show fabric route linkinfo
Rbridge-id: 1
===============
Reachable:    Yes
Version:      1
No. of Links: 2
```

```
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       1        Fi 1/-/-      128      Fi 2/-/-       10000       Pt_Pt
2       159      Fi 1/-/-      128      Fi 160/-/-     10000       Pt_Pt

Rbridge-id: 2
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       129      Fi 2/-/-      49       Fi 66/0/1      10000       Pt_Pt
2       128      Fi 2/-/-      1        Fi 1/-/-       10000       Pt_Pt

Rbridge-id: 65
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       2        Te 65/0/2     2        Te 66/0/2      500         Pt_Pt Ethernet   Yes
2       44       Te 65/0/44    20       Te 66/0/20     500         Pt_Pt Ethernet   Yes

Rbridge-id: 66
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       2        Te 66/0/2     2        Te 65/0/2      500         Pt_Pt Ethernet   Yes
2       20       Te 66/0/20    44       Te 65/0/44     500         Pt_Pt Ethernet   Yes
3       49       Fi 66/0/1     129      Fi 2/-/-       500         Pt_Pt            Yes
4       54       Fi 66/0/6     129      Fi 160/-/-     500         Pt_Pt            Yes

Rbridge-id: 160
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       129      Fi 160/-/-    54       Fi 66/0/6      10000       Pt_Pt
2       128      Fi 160/-/-    159      Fi 1/-/-       10000       Pt_Pt
```

See Also show fabric route topology, show fabric route neighbor-state

show fabric route multicast

Displays ISLs that receives any forwarded broadcast, unknown unicast, and multicast (BUM) traffic.

Synopsis **show fabric route multicast** [*rbridge-id* | *all*]

Operands

rbridge-id	**Specifies the ID of the routing bridge. This is not valid in standalone mode.**
all	Specifies all switches in the fabric.

Defaults None

Command Modes Privileged EXEC mode

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. The command displays the following fields:

Rbridge-id	Rbridge-id of the switch. The range of valid values is from 1 through 239.
Mcast Priority	Mcast priority value of the switch. The range of valid values is from 1 through 255.
Enet IP Addr	The switch Ethernet IP address.
WWN	World Wide Name of the switch.
Name	Switch name.
Src-Index	Source index of the local Rbridge.
Src-Port	Source port of the local rbridge in the format "local-rbridge-id/slot/port".
Nbr-Index	Neighbor Index of the ISL connected from local port.
Nbr-Port	Neighbor port of the ISL conncted from the local rbridge in the format "nbr-rbridge-id/slot/port".

Usage Guidelines This command is not available in standalone mode. If this command is executed without operands, it displays the multicast information of the local rbridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples To display the multicast routing information for all ports in the switch:

```
switch# show fabric route multicast
Root of the Multicast-Tree
==========================
Rbridge-id: 1
Mcast Priority: 1
Enet IP Addr: 10.24.85.212
WWN: 10:00:00:05:1e:cd:73:fa
Name: switch
Rbridge-id: 1
Src-Index    Src-Port     Nbr-Index    Nbr-Port    BW      Trunk
------------------------------------------------------------------
```

```
7           Te 1/0/7        55      Te 22/0/55   40G      Yes
15          Te 1/0/15       57      Te 23/0/57   60G      Yes
22          Te 1/0/22       58      Te 24/0/58   40G      Yes
26          Te 1/0/26       56      Te 25/0/56   60G      Yes
34          Te 1/0/34       58      Te 26/0/58   60G      Yes
41          Te 1/0/41       59      Te 27/0/59   20G      Yes
44          Te 1/0/44       56      Te 28/0/56   60G      Yes
```

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

show fabric route neighbor-state

Displays the state information of all the ISL links connected to the rbridge.

Synopsis **show fabric route neighbor-state** [**rbridge-id** *rbridge-id* | **all**]

Operands

rbridge-id *rbridge-id*	Specifies the ID of a routing bridge for which neighbor information is to be displayed. If no routing bridge is specified the neighbor state information for the local switch is displayed.
all	Displays neighbor information for all routing bridges in the fabric.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays information about neighbors to a specified routing bridge. FSPF defines a neighbor as a remote ISL interface that is directly attached to the local routing bridge. If the interfaces are trunked, the command displays data only about the trunk primary.

The command displays the following fields:

Rbridge-id	ID of the routing bridge. The range of valid values is from 1 through 239.
# ISLs	The number of ISLs that connect the switch to neighbor switches.
Src Index	E_Port interface on the local switch. This value is typically equal to the Index field reported in the **switchShow** command.
Src Interface	Physical interface on the local switch in the format "**Te** *rbridge-id/slot/port*". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	E_Port interface on the remote switch. This value is typically equal to the index field reported in the **switchShow** command.
Nbr Interface	Physical interface on the remote switch in the format "**Te** *rbridge-id/slot/port*". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr State	The FSPF neighbor state for the port attached to remote switch. The neighbor can be in one of the following states: **NB_ST_DOWN**—The neighbor is down. **NB_ST_INIT**—The neighbor is initializing. **NB_ST_DB_EX**—The neighbor and the switch are exchanging data from their Link State Records (LSR) databases. **NB_ST_DB_ACK_WT**—The neighbor is waiting for the switch to acknowledge the LSR database. **NB_ST_DB_WT**—The LSR Database is in waiting state; synchronization is in process. **NB_ST_FULL**—The neighbor is in the last, finishing state. The E_Port can route frames only if the neighbor is in full state.

Usage Guidelines If no information is available for the switch, the command displays the message “No ISL found.”

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples To display the state of FSPF neighbors for the local switch:

```
switch# show fabric route neighbor-state
Rbridge-id: 66   #ISLs: 8

 Src     Src              Nbr      Nbr            Nbr
Index   Interface        Index  Interface        State
-----------------------------------------------------
2       Te 66/0/2        2      Te 65/0/2       NB_ST_FULL
17      Te 66/0/17       41     Te 65/0/41      NB_ST_FULL
18      Te 66/0/18       42     Te 65/0/42      NB_ST_FULL
19      Te 66/0/19       43     Te 65/0/43      NB_ST_FULL
20      Te 66/0/20       44     Te 65/0/44      NB_ST_FULL
23      Te 66/0/23       47     Te 65/0/47      NB_ST_FULL
49      Fi 66/0/1        129    Fi 2/-/-        NB_ST_FULL
53      Fi 66/0/5        129    Fi 160/-/-      NB_ST_FULL
```

See Also **show fabric route topology, show fabric route linkinfo**

show fabric route pathinfo

Displays the path of a datastream through a fabric and provides statistics about each hop on that path.

Synopsis **show fabric route pathinfo**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command displays detailed routing information and statistics for a data stream from a source port on the local switch to a destination port on another switch. The destination switch can be a member of the same Brocade VCS Fabric cluster, a member of a different Brocade VCS Fabric cluster, a member of a Fabric OS backbone fabric, or a member of a Fabric OS edge fabric. This routing information describes the exact path that a user data stream takes to go from the source port to the destination port.

Use this command to check whether a congested link might be causing performance degradation on a specific data stream or path.

Select options interactively. The command prompts you for the following parameters:

Fabric ID Enter the VCS ID of the destination Network OS switch or the Fabric ID of the destination Fabric OS switch. If unspecified, the value defaults to -1, which specifies the Brocade VCS Fabric cluster of the local switch.

Domain Enter the routing bridge ID of the destination Network OS switch or the domain ID of the destination Fabric OS switch. You must enter a value for this parameter. It has no default value.

Source Port Enter the port index of the port at the head of the data stream to be traced. traced. If unspecified, the value defaults to -1, which specifies the embedded port.

Destination Port Enter the port index of the port on the destination switch for the path being traced. If unspecified, the value defaults to -1, which specifies the embedded port. The command output also reports the status of the Destination Port. If the specified port is out of range on the destination switch, the command fails with the message “Target port not present.”

Basic Stats Enter **y** to display basic statistics about each hop. By default, basis statistics are not displayed.

Extended Stats Enter **y** to display extended statistics about each hop. By default, extended statistics are not displayed.

Reverse Path Enter **y** to display reverse path information in addition to the forward path information. By default, reverse path information is not displayed.
The path from port A on switch X to port B on switch Y might be different from the path from port B to port A depending on the links traversed between a given sequence of switches, or the reverse path might involve different switches.

Regardless of option selection, the command displays the following status of the destination port and routing information about each hop:

Target port is	Provides the status of the destination port. It can have one of the following values: **Embedded**—This is the embedded port. **Not active**—The port is not connected or is still initializing and has not yet reached a stable state. **E_Port** **F_Port**
Hop	The hop number. The local switch is hop 0.
In Port	The port index of the port that the frames come in from on this path. For hop 0, this is the source port.
Domain ID	Routing bridge ID of the Network OS switch or domain of the Fabric OS switch.
Out Port	The port index of the port that the frames use to reach the next hop on this path. For the last hop, this is the destination port.
BW	The bandwidth of the output ISL in Gbps. It does not apply to the embedded port.
Cost	The cost of the ISL used by the fabric shortest path first (FSPF) routing protocol. It applies only to an E_Port.

You can request statistics for each hop in addition to the routing information. These statistics are presented for the input and output ports for both receive and transmit modes. You can select basic statistics, extended statistics, or both. Statistics are not reported for the embedded port. Some throughput values are reported in multiple time intervals to describe current path utilization and the average throughput over a longer period of time.

To collect these statistics, this command uses a special frame that is sent hop-by-hop from the source switch to the destination switch. To prevent such a frame from looping forever if an error occurs, a maximum of 25 hops is enforced. The hop count includes all hops in the direct path from source to destination, and also all the hops in the reverse path, if the tracing of the reverse path is requested. If the hop limit is exceeded, information collected up to the switch that returned the error is displayed along with the message “Maximum hops exceeded.”

If basic statistics are requested, the following information is provided for each hop in addition to the routing information:

B/s (1s)	Bytes per second transmitted and received over the previous 1 second period for the in port and for the out port.
B/s (64s)	Bytes per second transmitted and received over the previous 64 second period for the in port and for the out port.
TxCrdz(1s)	The length of time, in milliseconds, over the previous one second interval that the port was unable to transmit frames because the transmit BB credit was zero. The purpose of this statistic is to detect congestion or a device affected by latency. This parameter is sampled at 1 millisecond intervals,

and the counter is incremented if the condition is true. Each sample represents 1 ms of time with zero Tx BB Credit. An increment of this counter means that the frames could not be sent to the attached device for 1 ms, indicating degraded performance.

TxCrdz(64s) The length of time, in milliseconds, over the previous 64 second interval that the port was unable to transmit frames because the transmit BB credit was zero.

If extended statistics are requested, the following information is provided for each hop in the data path:

F/s (1s) The number of frames received or transmitted per second over the previous 1 second period.

F/s (64s) The number of frames received or transmitted per second over the previous 64 second period.

Words The total number of 4-byte Fibre Channel words.

Frames The total number of frames.

Errors The total number of errors that may have caused a frame not to be received correctly. This includes cyclic redundancy check (CRC) errors, bad end-of-frame (EOF) errors, frame truncated errors, frame-too-short errors, and encoding errors inside a frame.

Usage Guidelines

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples

To show path information without statistics or reverse path information:

```
switch# show fabric route pathinfo
Fabric ID (1..128)[-1]    : 10
Domain    : 1
Source Port [-1]    :
Destination Port [-1]    :
Basic Stats [y/n/yes/no]?    : n
Extended Stats [y/n/yes/no]?    : n
Reverse Path[y/n/yes/no]?    : n

------------------------------------------------------------------------
Target port is Embedded

Hop       In Port            Domain ID          Out Port    BW      Cost
------------------------------------------------------------------------
  0         E                   152               1        10G       500

  1         5                   142              54         4G       500

  2        14                     5               1         4G     10000

  3       217                   100             793        48G       500

  4      1209                     2             148         8G       500

  5         3                     1               E        --        --
```

To show path information with basic statistics:

```
switch# show fabric route pathinfo
Fabric ID (1..128)[-1]    : 10
Domain    : 1
Source Port [-1]    :
Destination Port [-1]    :
Basic Stats [y/n/yes/no]?    : y
Extended Stats [y/n/yes/no]?    : n
Reverse Path[y/n/yes/no]?    : n

------------------------------------------------------------------------
Target port is Embedded

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  0         E                   152              1         10G      500

Port                        E                            1
                  ------------------------------------------------------
                        Tx              Rx              Tx              Rx
B/s (1s)                --              --               0               0
B/s (64s)               --              --               0               0
TxCrdz (1s)             --              --               0              --
TxCrdz (64s)            --              --               0              --

Hop       In Port            Domain ID           Out Port     BW     Cost
------------------------------------------------------------------------
  1         5                   142              54           4G      500

Port                            5                       54
                       Tx              Rx              Tx              Rx
                       ------------------------------------------------
B/s (1s)                0               0               0               0
B/s (64s)               0               0               7               7
TxCrdz (1s)             0               --              0              --
TxCrdz (64s)            0               --              0              --

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  2        14                    5               1          4G    10000

Port                            14                      1
                       Tx              Rx              Tx              Rx
                       ------------------------------------------------
B/s (0s)                0               0               0               0
B/s (0s)                0               0               0               0
TxCrdz (0s)             0               --              0              --
TxCrdz (0s)             0               --              0              --

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  3       217                 100              793        48G      500
Port                          217                         793
                       Tx              Rx              Tx              Rx
                       ------------------------------------------------
B/s (1s)                0               0               0               0
B/s (64s)               4               4               0               0
TxCrdz (1s)             0               --              0              --
TxCrdz (64s)            0               --              0              --
```

```
Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  4      1209                   2              148         8G      500

Port                           1209                   148
                      Tx              Rx              Tx              Rx
                      ------------------------------------------------
B/s (1s)               0               0               0               0
B/s (64s)              0               0               3               0
TxCrdz (1s)            0              --               0              --
TxCrdz (64s)           0              --               0              --

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  5         3                   1                E        --      --

Port                           3                      E
                      Tx              Rx              Tx              Rx
                      ------------------------------------------------
B/s (1s)               0               0              --              --
B/s (64s)              0               3              --              --
TxCrdz (1s)            0              --              --              --
TxCrdz (64s)           0              --              --              --
```

To show path information with extended statistics and reverse path information:

```
switch# show fabric route pathinfo
Fabric ID (1..128)[-1]    : 10
Domain    : 1
Source Port [-1]    :
Destination Port [-1]    :
Basic Stats [y/n/yes/no]?    : y
Extended Stats [y/n/yes/no]?    : y
Reverse Path[y/n/yes/no]?    : y

---------------------------------------------------------------
Target port is Embedded

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  0         E                  152               1        10G      500

Port                       E                                 1

                    Tx              Rx                Tx              Rx
                    ------------------------------------------------
B/s (1s)            --              --                 0               0
B/s (64s)           --              --                 0               0
TxCrdz (1s)         --              --                 0              --
TxCrdz (64s)        --              --                 0              --
F/s (1s)            --              --                 0               0
F/s (64s)           --              --                 0               0
Words               --              --                 0               0
Frames              --              --                 0               0
Errors              --              --                --               0

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  1        5                  142               54        4G      500
```

```
Port                          5                          54
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              0               0               0               0
B/s (64s)             0               0               7               7
TxCrdz (1s)           0               --              0               --
TxCrdz (64s)          0               --              0               --
F/s (1s)              0               0               0               0
F/s (64s)             0               0               0               0
words                 0               0             967             967
Frames                0               0            1204             967
Errors                --              0              --               0

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  2        14                   5                  1         4G    10000

Port                          14                        1
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (0s)              0               0               0               0
B/s (0s)              0               0               0               0
TxCrdz (0s)           0               --              0               --
TxCrdz (0s)           0               --              0               --
F/s (0s)              0               0               0               0
F/s (0s)              0               0               0               0
words
Frames
Errors                --              0               --              0

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  3       217                  100                793       48G      500

Port                          217                       793
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              0               0               0               0
B/s (64s)             4               4               0               0
TxCrdz (1s)           0               --              0               --
TxCrdz (64s)          0               --              0               --
F/s (1s)              0               0               0               0
F/s (64s)             0               0               0               0
words             50570           50570       511118479       511118479
Frames            50742           50570       539255694       511118479
Errors                --              0               --              0

Hop       In Port            Domain ID        Out Port      BW     Cost
------------------------------------------------------------------------
  4        1209                  2             148        8G      500

Port                          1209                      148
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              0               0               0               0
B/s (64s)             0               0               3               0
TxCrdz (1s)           0               --              0               --
TxCrdz (64s)          0               --              0               --
F/s (1s)              0               0               0               0
```

```
F/s (64s)              0               0               0               0
words                608             608             424             424
Frames               454             608             563             424
Errors                --               0              --               0

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  5         3                    1                E         --       --

Port                            3                       E
                      Tx              Rx              Tx              Rx
                      ------------------------------------------------
B/s (1s)               0               0              --              --
B/s (64s)              0               3              --              --
TxCrdz (1s)            0              --              --              --
TxCrdz (64s)           0              --              --              --
F/s (1s)               0               0              --              --
F/s (64s)              0               0              --              --
words               1244            1244              --              --
Frames               898            1244              --              --
Errors                --               0              --              --

        Reverse Path
Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  6         E                    1                0          8G      500

Port                            E                       0
                      Tx              Rx              Tx              Rx
                      ------------------------------------------------
B/s (1s)              --              --               0               0
B/s (64s)             --              --               4               4
TxCrdz (1s)           --              --               0              --
TxCrdz (64s)          --              --               0              --
F/s (1s)              --              --               0               0
F/s (64s)             --              --               0               0
Words                 --              --             809             809
Frames                --              --            1645             809
Errors                --              --              --               0

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  7       149                  2               1204       48G      500

Port                          149                     1204
                      Tx              Rx              Tx              Rx
                      ------------------------------------------------
B/s (1s)               0               0               0               0
B/s (64s)              4               4               0               0
TxCrdz (1s)            0              --               0              --
TxCrdz (64s)           0              --               0              --
F/s (1s)               0               0               0               0
F/s (64s)              0               0               0               0
words                707             707              56              56
Frames               403             707              57              56
Errors                --               0              --               0

Hop       In Port            Domain ID           Out Port    BW     Cost
------------------------------------------------------------------------
  8        796                 100              217        4G      500
```

```
Port                          796                   217
                        Tx             Rx             Tx             Rx
                        ------------------------------------------------
B/s (1s)                0              0              0              0
B/s (64s)               0              0              4              4
TxCrdz (1s)             0             --              0             --
TxCrdz (64s)            0             --              0             --
F/s (1s)                0              0              0              0
F/s (64s)               0              0              0              0
words            48267544       48267544          50570          50570
Frames            1164982       48267544          50742          50570
Errors                 --              0             --              0
```

See Also show fabric route topology, show fabric route neighbor-state

show fabric route topology

Displays the RBridge routes from the source switch to the destination switch.

Synopsis **show fabric route topology** [**src-rbridgeId** *src-id*] [**dst-rbridgeId** *dst_id*]

Operands

src-rbridgeId	The source routing bridge (RBridge)
src-id	**Specifies** details on the source RBridge.
dst-rbridgeId	The destination RBridge
dst_id	**Specifies** details on the destination RBridge.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Description Use this command to display the Rbridge routes to other switches. The command displays the following fields:

Path Count	The number of currently active paths to the destination domain
Src RB-ID	Rbridge-id of the switch. The range of valid values is from 1 through 239.
Dst RB-ID	Destination rbridge-id to where the traffic flows. The range of valid values is from 1 through 255.
Out Index	The port index to which incoming frames are forwarded to reach the destination rbridge.
Out Interface	The port interface (local-rbridge-id/slot/port") of the local rbridge to which incoming frames are forwarded to the destination rbridge. If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Hops	The maximum number of hops to reach destination rbridge.
Cost	The cost of reaching destination domain.
Nbr Index	Neigbor Index of the ISL connected from local port.
Nbr Interface	Neighbor interface of the ISL conncted from the local rbridge in the format "nbr-rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
BW	Bandwidth of the traffic.
Trunk	Displays "Yes" if trunk is enabled in the ISL.

Usage Guidelines The RBridge routes to other switches are the available paths to remote domains that unicast traffic can take.

This command is not available in standalone mode.

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.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples To display the fabric route topology information:

```
switch# show fabric route topology
Total Path Count: 3
Src    Dst    Out    Out                      Nbr    Nbr
RB-ID  RB-ID  Index  Interface   Hops  Cost  Index  Interface   BW   Trunk
------------------------------------------------------------------------------
  1       2       2    Te 1/0/2     2    1000   56    Te 21/0/56  60G   Yes
  2       26   Te 1/0/26    2    1000   56    Te 25/0/56  60G   Yes
  2       44   Te 1/0/44    2    1000   56    Te 28/0/56  60G   Yes
  2       15   Te 1/0/15    2    1000   57    Te 23/0/57  60G   Yes
  2       34   Te 1/0/34    2    1000   58    Te 26/0/58  60G   Yes
  2       7    Te 1/0/7     2    1000   55    Te 22/0/55  40G   Yes
  2       22   Te 1/0/22    2    1000   58    Te 24/0/58  40G   Yes
  2       37   Te 1/0/37    2    1000   56    Te 27/0/56  40G   Yes
  2       12   Te 1/0/12    2    1000   60    Te 22/0/60  20G   Yes
  2       41   Te 1/0/41    2    1000   59    Te 27/0/59  20G   Yes
  2       20   Te 1/0/20    2    1000   56    Te 24/0/56  10G   Yes
  21      2    Te 1/0/2     1    500    60    Te 21/0/56  60G   Yes
  22      7    Te 1/0/7     1    500    55    Te 22/0/55  40G   Yes
  22      12   Te 1/0/12    1    500    60    Te 22/0/60  20G   Yes
  23      15   Te 1/0/15    1    500    57    Te 23/0/57  60G   Yes
  24      22   Te 1/0/22    1    500    58    Te 24/0/58  40G   Yes
  24      20   Te 1/0/20    1    500    56    Te 24/0/56  10G   Yes
  25      26   Te 1/0/26    1    500    56    Te 25/0/56  60G   Yes
  26      34   Te 1/0/34    1    500    58    Te 26/0/58  60G   Yes
  27      37   Te 1/0/37    1    500    56    Te 27/0/56  40G   Yes
  27      41   Te 1/0/41    1    500    59    Te 27/0/59  20G   Yes
```

See Also **fabric route mcast**

show fabric trunk

Displays interswitch (ISL) trunk information.

Synopsis **show fabric trunk** [*rbridge-id* | *all*]

Operands

rbridge-id	**Specifies the ID of the routing bridge. This is not valid in standalone mode.**
all	Specifies all switches in the fabric.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Description Use this command to display trunking information of ISL ports. The command displays the following fields:

Rbridge-id	Rbridge-id of the switch. The range of valid values is from 1 through 239.
Trunk Group	Displays each trunking group on a switch. All ports that are part of this trunking group are displayed.
Src Index	Source index of the local Rbridge.
Src Interface	Source interface of the local rbridge in the format “local-rbridge-id/slot/port”. If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	Neighbor Index of the ISL connected from local port. If the link is segmented and the NBR rbridge details are unavailable, "?" displays in this field.
Nbr Interface	Neighbor interface of the ISL connected from the local rbridge in the format “nbr-rbridge-id/slot/port”. If the ISL is not completely up, this field will be displayed as "?/?/?". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr-WWN	Neighbor WWN of the switch. If the ISL is segmented and the neighbor rbridge details are not available, then "??:??:??:??:??:??:??:??" displays in this field.

Usage Guidelines This command is not available in standalone mode. If this command is executed without operands, it displays the trunk information of the local rbridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level rbridge.

Examples To display the fabric trunk information:

```
switch# show fabric trunk
Possible completions:
  all         all RBridges in fabric
  rbridge-id   Syntax: rbridge-id [rbridge-id]
  |           Output modifiers
  <cr>
```

```
switch# show fabric trunk
Rbridge-id: 65

Trunk  Src    Source          Nbr     Nbr
Group  Index  Interface       Index   Interface       Nbr-WWN
------------------------------------------------------------------------
1      1      Te 65/0/1       1       Te 66/0/1       10:00:00:05:33:6F:27:57
1      2      Te 65/0/2       2       Te 66/0/2       10:00:00:05:33:6F:27:57
2      45     Te 65/0/45      21      Te 66/0/21      10:00:00:05:33:6F:27:57
2      47     Te 65/0/47      23      Te 66/0/23      10:00:00:05:33:6F:27:57
2      46     Te 65/0/46      22      Te 66/0/22      10:00:00:05:33:6F:27:57
```

See Also fabric trunk enable, show fabric isl, show fabric islports

show fabric vlag-load-balance

Displays the fabric VLAG load-balance information.

Synopsis **show fabric vlag-load-balance** [*port-channel-id* | **all**]

Operands

port-channel-id	The port channel ID.
all	Displays all of the information

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the fabric VLAG load-balance information.

Usage Guidelines None

Examples

```
switch# show fabric vlag-load-balance 10
Fabric Vlag Load-Balance Information
------------------------------
Rbridge-Id               : 2
Vlag                         : 10
Load-Balance Flavor : Source and Destination MAC address and VID based load
balancing

switch# show fabric vlag-load-balance all
Fabric Vlag Load-Balance Information
------------------------------
Rbridge-Id                : 2
Vlag                           : 10
Load-Balance Flavor   : Source and Destination MAC address and VID based load
balancing
Vlag                           : 20
Load-Balance Flavor   : Destination MAC address and VID based load balancing
```

See Also **show running-config rbridge-id**

show fcoe fabric-map

Displays the current configuration of the FCoE fabric-map.

Synopsis **show fcoe fabric-map** [**default** {**rbridge-id** *rbridge-id*} | **rbridge-id** *rbridge-id*]

Operands

default The fabric map name. The only map name available is “default”.

rbridge-id *rbridge-id*
Specifies the ID of the routing bridge.

rbridge-id *rbridge-id* Specifies the ID of the routing bridge.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the current configuration of the FCoE fabric-map.

Usage Guidelines This command is not available in standalone mode.

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
```

See Also None

show fcoe interface

Displays a synopsis of the FCoE interfaces.

Synopsis **show fcoe interface** [**brief** | **ethernet rbridge-id** *rbridge-id*]

Operands

brief	Displays a brief synopsis of the configuration status
ethernet	Displays the FCoE Ethernet Interface information.
rbridge-id *rbridge-id*	Specifies the ID of the routing bridge.

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 This command is not available in standalone mode.

Examples

```
switch# show fcoe interface brief
================================================================================
FCOE IF             Mode            Status       Binding          Num
               Config Current  Config     Proto                VN Ports
================================================================================
1/12/1         VF     VF       Up         Down   Te 12/0/1      0
1/12/2         VF     VF       Up         Down   Te 12/0/2      0
1/12/3         VF     VF       Up         Down   Te 12/0/3      0
1/12/4         VF     VF       Up         Down   Te 12/0/4      0
1/12/5         VF     VF       Up         Down   Te 12/0/5      0
1/12/6         VF     VF       Up         Down   Te 12/0/6      0
1/12/7         VF     VF       Up         Down   Te 12/0/7      0
1/12/8         VF     VF       Up         Down   Te 12/0/8      0
1/12/9         VF     VF       Up         Down   Te 12/0/9      0
1/12/10        VF     VF       Up         Down   Te 12/0/10     0
1/12/11        VF     VF       Up         Down   Te 12/0/11     0
1/12/12        VF     VF       Up         Down   Te 12/0/12     0
1/12/13        VF     VF       Up         Down   Te 12/0/13     0
1/12/14        VF     VF       Up         Down   Te 12/0/14     0
1/12/15        VF     VF       Up         Down   Te 12/0/15     0
```

See Also None

show fcoe login

Displays FCoE login information.

Synopsis **show fcoe login** {**interface** [**WORD** | **VN-Num** | **Rbridge** | **port**]} {**rbridge-id** *rbridge-id*} {**vfid** *value*} {**vlan** *value*}

Operands

interface	Show Logins for an FCoE interface
WORD	Displays Word information.
VN-Num	Displays VN-Num information.
Rbridge	Displays Rbridge information.
port	Displays port information.
rbridge-id *rbridge-id*	Show FCoE logins for a given RbridgeID.
vfid *value*	Show Logins for a Virtual Fabric. The range of valid values is from 1 through 4096.
vlan *value*	Show Logins for an FCoE VLAN. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays FCoE login information.

Usage Guidelines This command is not available in standalone mode.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples None

See Also None

show fcoe map

Displays all FCoE maps, or a single map.

Synopsis **show fcoe map** [**default** {**rbridge-id** *rbridge-id*} | **rbridge-id** *rbridge-id*]

Operands

default	The fabric map name. The only map name available is “default”.
rbridge-id *rbridge-id*	Specifies the ID of the routing bridge.
rbridge-id *rbridge-id*	Specifies the ID of the routing bridge.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays all available FCoE maps, or a single designated map. However, for Network OS v3.0.0, the only map name allowed is “default.”

Usage Guidelines None

This command is not available in standalone mode.

Examples

```
switch#show fcoe map default
===============================================================
Name                DCB-Map         FABRIC-MAP(s)
===============================================================
default             default         default
```

See Also None

show fcsp auth-secret dh-chap

Displays the switches (WWNs) for which a shared secret is configured

Synopsis **show fcsp auth-secret dhchap**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the switch world wide names (WWNs) for which a shared secret is configured.

Usage Guidelines This command is supported only on the Brocade VDX 6730 platforms.

Examples

```
switch# show fcsp auth-secret dh-chap
 10:00:00:05:1e:7a:c3:00
```

See Also **fcsp auth, fcsp auth-secret, show running-config fcsp auth**

show file

Displays the contents of a file.

Synopsis **show file** *filename*

Operands

filename	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-copy
diag post rbridge-id 237
 no enable
!
linecard 2 LC48x10G
linecard 4 LC48x10G
class-map default
 match any
!
logging rbridge-id 237
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
switch-attributes 237
 chassis-name VDX8770-4
 host-name sw0
!
support rbridge-id 237
 ffdc
!
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server host 172.26.3.84 public
 udp-port 5000
 severity-level Info
!
[output truncated]
```

See Also copy, delete, dir, rename

show fips

Displays the current FIPS configuration.

Synopsis **show fips**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display whether FIPS self tests are enabled, and whether the root account is disabled.

Usage Guidelines None

Examples To display the FIPS enabled status:

```
switch# show fips
FIPS Selftests: Enabled
Root account:   Disabled
```

See Also fips root disable, fips selftests, fips zeroize, prom-access disable, unhide fips

show firmwaredownloadhistory

Displays the history of firmware downloads.

Synopsis **show firmwaredownloadhistory** [**rbridge-id** {*rbridge-id* | **all**}*]*

Operands

rbridge-id	Executes the command on the specified switch.
rbridge-id	Specifies the unique identifier for the switch.
all	Executes the command on all switches in the cluster

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the firmware download history log. The log records the date and time of the firmware download, the switch name, slot number, process ID and firmware version.

Usage Guidelines This command displays information for the local management module only. The **rbridge-id** and **all** operands are not supported.

Examples To display the firmware download history:

```
switch# show firmwaredownloadhistory

Firmware version history

Sno  Date & Time                   Switch Name  Slot  PID    OS Version
1    Thu Feb  2 10:40:22 2012      sw0          0     1561   nos3.0.0
2    Tue Jan 31 11:47:59 2012      testA1-sw0   0     1551   nos2.1.1
```

See Also **firmware commit, firmware download, show version**

show firmwaredownloadstatus

Displays the firmware download activity log.

Synopsis **show firmwaredownloadstatus** [**brief**] [**rbridge-id** {*rbridge-id* | **all**}*]*

Operands

brief	**Displays only the last entry of the firmware download event log.**
rbridge-id	Executes the command on the specified switch.
rbridge-id	Specifies the unique identifier for the switch.
all	Specifies all switches in the VCS 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 retained until you issue another **firmware download** command. A time stamp is associated with each event.

Usage Guidelines The **rbridge-id** and **all** operands are not supported.

The output varies depending on the hardware platform.

Examples To display the firmware download event log on the Brocade VDX 8770-4:

```
switch# show firmwaredownloadstatus
[1]: Tue Mar  6 04:05:20 2012
Slot M1: Firmware install begins.

[2]: Tue Mar  6 04:09:02 2012
Slot M1: Firmware install ends.

[3]: Tue Mar  6 04:09:02 2012
Slot M2: Firmware install begins.

[4]: Tue Mar  6 04:12:08 2012
Slot M2: Firmware install ends.

[5]: Tue Mar  6 04:12:09 2012
Slot M1: Firmware starts to swap.

[6]: Tue Mar  6 04:12:09 2012
Slot M2: Firmware starts to swap.
 (output truncated)
```

To display a condensed version of the firmware download status:

```
switch# show firmwaredownloadstatus brief

[35]: Tue Mar  6 04:23:10 2012
Slot M1: Firmware is downloaded successfully.
```

See Also **firmware commit, firmware download, firmware restore, show version**

show ha

Displays the High Availability (HA) status of the management modules.

Synopsis **show ha [all-partition]**

Operand

all-partition	Displays the HA status for all partitions.

Defaults Displays the HA status for the management modules.

Command Modes Privileged EXEC mode

Description Use this command to display the HA status of the management modules. The display includes the following information:

- Local MM state: warm or cold, recovering or recovered
- Remote MM state: warm or cold, recovering or recovered, or not available
- High Availability (enabled or disabled).
- Heartbeat (up or down).
- Health of standby management module
- HA synchronization status

The health of the standby CP is defined as follows:

Healthy	The standby management module is running and the background health diagnostic has not detected any errors.
Failed	The standby is running, but the background health diagnostic has discovered a problem with the blade. Check the logs to determine the appropriate action.
Unknown	The standby management module's health state is unknown because of one of the following reasons: the standby CP does not exist, Heartbeat is down, or the Health Monitor has detected a configuration file error.

The High Availability synchronization status is defined as follows:

HA State synchronized	The system is fully synchronized. If a failover becomes necessary, it is nondisruptive.
HA State not in sync	The system is unable to synchronize the two management modules. This may be caused by one or more of the following conditions: A failover is in process but not completed The standby management module is faulty. A system error occurred.

If a failover becomes necessary while the management modules are not in sync, the standby management module reboots, and the failover is disruptive.

Usage Guidelines HA is not supported in this release. All failover is disruptive. The HA commands are provided for consistency and future expansion.

Examples To display HA status:

```
switch# show ha
Local (M2): Active, Cold Recovered
Remote (M1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

See Also ha enable, ha disable, ha failover

show interface

Displays the detailed interface configuration and capabilities of all interfaces or for a specific interface.

Synopsis **show interface** {**port-channel** *number* | **tengigabitethernet** *rbridge-id/slot/port* | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **switchport** | **tracked** | **fcoe** *rbridge-id/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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
fortygigabitethernet	Specifies a valid 40 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface
rbridge-id	Specifies a switch by its RBridge identifier.
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 *rbridge-id/slot/port*	Displays the FCoE information for the designated interface.
vlan *vlan_id*	Specifies which VLAN interface to display. Refer to "Usage Guidelines" below.

Defaults None

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 The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To display detailed information for 10 Gbps Ethernet interface 1/0/1:

```
switch#show interface tengigabitethernet 1/0/1
TenGigabitEthernet 1/0/1 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 detailed information for a 1 Gbps interface on a Brocade VDX 6710 switch:

```
switch#show interface gigabitethernet 1/0/2
GigabitEthernet 1/0/2 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.1e76.1aa5
    Current address is 0005.3313.ac7f
Fixed copper RJ-45 media present
Interface index (ifindex) is 4697661440
MTU 2500 bytes
LineSpeed: 1000 Mbit, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 1d12h37m
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:
```

```
    4425 packets, 513300 bytes
    Unicasts: 4425, 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: 15:14:13
```

To display Layer 2 information for all interfaces:

```
switch#show interface switchport

 Interface name          : TenGigabitEthernet 1/0/8
 Switchport mode         : access
 Ingress filter          : enable
 Acceptable frame types  : all
 Default Vlan            : 1
 Active Vlans            : 1
 Inactive Vlans          : -

 Interface name          : TenGigabitEthernet 1/0/19
 Switchport mode         : hybrid
 Ingress filter          : enable
 Acceptable frame types  : all
 Default Vlan            : 1
 Active Vlans            : 1
 Inactive Vlans          : 100

 Interface name          : TenGigabitEthernet 1/0/20
 Switchport mode         : trunk
 Ingress filter          : enable
 Acceptable frame types  : vlan-tagged only
 Default Vlan            : 0
 Active Vlans            : 1
 Inactive Vlans          : -
```

See Also show ip interface

show interface FibreChannel

Displays Fibre Channel port hardware statistics.

Synopsis **show interface FibreChannel** *rbridge-id/slot/port* [**detail**]

Operands

rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
detail	Displays detailed error and statistics counters.

Defaults None

Command Modes Privileged EXEC mode

Description This command reports the up or down status of the port, the up or down status of the Fibre Channel protocol, whether any pluggable media is present, and the following configuration information:

LineSpeed Actual	Operating speed of the port.
PortSpeed	Fixed speed of the port.
portDisableReason	The reason the port is disabled.
PortId	24-bit port ID.
PortIfId	24-bit port interface ID.
PortWwn	World wide name of the port.
Distance	Long-distance level of the port. In the case of LD mode, the user configured distance and actual distance are both displayed.

Following the general information, the command displays three columns of counters. The first column shows interrupt statistics:

Interrupts	Total number of interrupts.
Unknown	Interrupts that are not counted elsewhere.
Lli	Low-level interface (physical state, primitive sequences).
Proc_rqrd	Frames delivered for embedded N_Port processing.
Timed_out	Frames that have timed out.
Rx_flushed	Frames requiring translation.
Tx_unavail	Frames returned from an unavailable transmitter.
Free_buffer	Free buffer available interrupts.
Overrun	Buffer overrun interrupts.
Suspended	Transmission suspended interrupts.
Parity_err	Central memory parity errors.
2_parity_err	Secondary transmission parity errors.

The second column displays link error status block counters.

Link_failure	Link failures
Loss_of_sync	Synchronization losses
Loss_of_sig	Signal losses
Protocol_err	Protocol errors
Invalid_word	Invalid words
Invalid_crc	Cyclic redundancy errors
Delim_err	Delimiter errors
Address_err	Addressing errors
Lr_in	Line resets in
Li_out	Line resets out
Ols_in	Offline primitive sequences in
Ols_out	Offline primitive sequences out

The third column shows the number of transmitted frames rejected and busied:

Frjt	Transmitted frames rejected.
Fbsy	Transmitted frames busied.

finally, some transmission rate Information is displayed:

Bandwidth	Bandwidth of the port.
Tx performance	Bytes per second transmitted.
Rx performance	Bytes per second received

When used with the **detail** operand, this command also reports the following receive statistics, transmit statistics, error statistics, and port error information.

Receive statistics:

stat_wrx	4-byte words received.
stat_frx	Frames received.
stat_c2_frx	Class 2 frames received.
stat_c3_frx	Class 3 frames received.
stat_lc_rx	Link control frames received.
stat_mc_rx	Multicast frames received.

Transmit statistics:

stat_wtx	4-byte words transmitted.
stat_ftx	Frames transmitted.
stat_mc_tx	Multicast frames transmitted.

tim_txcrd_z	The number of times that the port was unable to transmit frames because the transmit buffer-to-buffer (BB) credit was zero. The purpose of this statistic is to detect congestion or a device affected by latency. This parameter is sampled at intervals of 2.5 microseconds, and the counter is incremented if the condition is true. Each sample represents 2.5 microseconds of time with zero Tx BB Credit. An increment of this counter means that the frames could not be sent to the attached device for 2.5 microseconds, indicating degraded performance.
Error statistics:	
er_enc_in	Encoding errors inside frames.
er_crc	Frames with cyclic redundancy check (CRC) errors.
er_trunc	Frames shorter than the minimum frame length.
er_toolong	Frames longer than the maximum frame length.
er_bad_eof	Frames with bad end-of-frame.
er_enc_out	Encoding error outside frames.
er_bad_os	Invalid ordered sets (platform-specific and port-specific).
er_rx_c3_timeout	Receive class 3 frames received at this port and discarded at the transmission port due to timeout (platform-specific and port-specific).
er_tx_c3_timeout	Transmit class 3 frames discarded at the transmission port due to timeout (platform-specific and port-specific).
er_c3_dest_unreach	Class 3 frames discarded because the transmit port, although it is determined, cannot send the frame at the moment when the error occurs.
er_other_discard	Other discards due to route lookup failures or other reasons.
er_type1_miss	FCR frames with transmit errors.
er_type2_miss	Frames with routing errors.
er_type6_miss	FCR frames with receive errors.
er_zone_miss	Frames discarded due to hard zoning miss. Hardware zoning enforcement is not supported currently.
er_lun_zone_miss	Frames discarded due to zoning miss. LUN zoning is not supported currently.
er_crc_good_eof	CRC errors with good end-of-frame (EOF).
er_inv_arb	Invalid ARBs.
Port error information:	
Loss_of_sync	Link synchronization errors.
Loss_of_sig	Link loss-of-signal errors.
Frjt	Transmitted frames rejected.
Fbsy	Transmitted frames busied.
Buffer information:	
Lx Mode	L0—Link not in long distance mode.

LD—Link is from 5 km through 10 km.

LE—Distance is determined dynamically.

LS—Distance is determined statically by user.

Max/Resv Buffers The maximum or reserved number of buffers that are allocated to the port based on the estimated distance (as defined by the **desire-distance** command). If the port is not configured in long distance mode, some systems might reserve buffers for the port. This field then displays the number of buffers reserved for the port.

Buffer Usage The actual number of buffers allocated to the port. In LD mode, the number is determined by the actual distance and the user-specified desired distance (as defined by the **desired-distance** command).

Needed Buffers The number of buffers needed to utilize the port at full bandwidth (depending on the port configuration). If the number of Buffer Usage is less than the number of Needed Buffers, the port is operating in the buffer limited mode.

Link Distance For L0 (not in long distance mode), the command displays the fixed distance based on port speed, for instance: 10 km (1 Gbps), 5 km (2 Gbps), 2 km (4 Gbps), or 1 km (8 Gbps). For static long distance mode (LE), the fixed distance of 10 km displays. For LD mode, Brocade switches use a proprietary algorithm to estimate distance across an ISL. LD mode supports distances up to 500 km. Distance measurement on a link longer than 500 km might not be accurate. If the connecting port does not support LD mode, is shows "N/A".

Remaining Buffers The remaining (unallocated and reserved) buffers in a port group.

A hyphen in one of the Buffer information display fields indicates that no relevant information is available; there may be no connection to a port, or the port is disabled, or the port is not an E_Port.

Usage Guidelines This command applies only to the Brocade VDX 6730 switches.

Examples To view Fibre Channel port statistics:

```
switch# show interface FibreChannel 66/0/1
fibrechannel 66/0/1 is up.  Protocol state is up (connected)
Pluggable media present
LineSpeed Actual:              400,800_MB/s
PortSpeed:                     N8Gbps
portDisableReason:             None
PortId:                        427900
PortIfId:                      4302303f
PortWwn:                       20:79:00:05:33:67:26:78
Distance:                      normal

Last clearing of show interface counters: 00:00:00
Interrupts:         0          Link_failure: 0          Frjt:
0
Unknown:            0           Loss_of_sync: 1          Fbsy:
0
Lli:               9          Loss_of_sig:  2
Proc_rqrd:         5          Protocol_err: 0
Timed_out:         0          Invalid_word: 0
Rx_flushed:        0          Invalid_crc:  0
```

```
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err:  0
Overrun:           0          Lr_in:        1
Suspended:         0          Lr_out:       1
Parity_err:        0          Ols_in:       0
2_parity_err:      0          Ols_out:      1

Rate info:
  Bandwidth:       8.00G
  Tx performance:  0 B/sec
  Rx performance:  0 B/sec
```

To view Fibre Channel port statistics details:

```
switch# show interface FibreChannel 66/0/1 detail
fibrechannel 66/0/1 is up.  Protocol state is up (connected)
Pluggable media present
LineSpeed Actual:               400,800_MB/s
portSpeed:                      N8Gbps
portDisableReason:              None
portId                          423100
portIfId:                       43020026
portWwn:                        20:31:00:05:33:6f:27:57
Distance                        normal

Last clearing of show interface counters: 00:00:00
Rx Statistics:
        stat_wrx                118         4-byte words received
        stat_frx                4           Frames received
        stat_c2_frx             0           Class 2 frames received
        stat_c3_frx             0           Class 3 frames received
        stat_lc_rx              2           Link control frames received
        stat_mc_rx              0           Multicast frames received
Tx Statistics:
        stat_wtx                282         4-byte words transmitted
        stat_ftx                12          Frames transmitted
        stat_mc_tx              0           Multicast frames transmitted
        tim_txcrd_z             2881        Time TX Credit Zero (2.5Us ticks)
        tim_txcrd_z_vc  0- 3:   2881        0           0           0
        tim_txcrd_z_vc  4- 7:   0           0           0           0
        tim_txcrd_z_vc  8-11:   0           0           0           0
        tim_txcrd_z_vc 12-15:   0           0           0           0
Error Statistics
        er_enc_in               0           Encoding errors inside of frames
        er_crc                  0           Frames with CRC errors
        er_trunc                0           Frames shorter than minimum
        er_toolong              0           Frames longer than maximum
        er_bad_eof              0           Frames with bad end-of-frame
        er_enc_out              0           Encoding error outside of frames
        er_bad_os               1           Invalid ordered set
        er_rx_c3_timeout        0           Class 3 receive frames discarded
due to timeout
        er_tx_c3_timeout        0           Class 3 transmit frames discarded
due to timeout
        er_c3_dest_unreach      0           Class 3 frames discarded due to
destination unreachable
        er_other_discard        0           Other discards
        er_type1_miss           0           frames with FTB type 1 miss
        er_type2_miss           0           frames with FTB type 2 miss
        er_type6_miss           0           frames with FTB type 6 miss
```

```
        er_zone_miss            0           frames with hard zoning miss
        er_lun_zone_miss        0           frames with LUN zoning miss
        er_crc_good_eof         0           Crc error with good eof
        er_inv_arb              0           Invalid ARB

Port Error Info:
        Loss_of_sync:1
        Loss_of_sig:2
        Frjt:0
        Fbsy:0

Buffer Information:
 Lx       Max/Resv    Buffer   Needed     Link        Remaining
 Mode     Buffers     Usage    Buffers    Distance    Buffers
================================================================
 -         8            0         0        -             924

Rate info:
  Bandwidth:       8.00G
  Tx performance:  0 B/sec
  Rx performance:  0 B/sec
```

See Also show running-config interface FibreChannel, interface

show interface management

Displays the management interfaces.

Synopsis **show interface management** [*rbridge-id/port*]

Operands

rbridge-id/port	Specifies the management interface to be configured as the *rbridge-id* followed by a slash (/) and the port number.
port	On standalone platforms, the port number for the management port is always 0. On a modular switches with two redundant management modules, can configure two management ports, 1 and 2.

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 The address field indicates if DCHP is used to obtain an IP address or if a static IP address is used.

Examples To display the management interface configured with an IPv4 address::

```
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"
```

To display the management interface configured with a static IPv6 address:

```
switch# show interface management
interface Management 1/0
 ip address 10.17.19.145/20
 ip gateway-address 10.17.16.1
 ipv6 ipv6-address [ "static aaaa::aaaa/64 preferred" ]
 ipv6 ipv6-gateways [ fe80::21b:edff:fe0b:3c00 fe80::21b:edff:fe0b:9000 ]
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
```

To display the management interfaces on a Brocade VDX 8770. Interface 1/1 is configured with stateless IPv6 addresses:

```
switch# show interface management
interface Management 1/1
 ip address 10.24.82.121/20
 ip gateway-address 10.24.80.1
 ipv6 ipv6-address [ "stateless fd00:60:69bc:64:205:33ff:fe15:f980/64
preferred" ]
 ipv6 ipv6-gateways [ fe80::21b:edff:fe0f:bc00 fe80::21b:edff:fe0c:c200 ]
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
interface Management 1/2
 ip address 10.24.82.255/20
```

```
    ip gateway-address 10.24.80.1
    ipv6 ipv6-address [  ]
    ipv6 ipv6-gateways [  ]
    line-speed actual "1000baseT, Duplex: Full"
    line-speed configured Auto
```

See Also interface management, show running-config interface management

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 None

Command Modes Privileged EXEC mode

Description Use this command to display the FIB information.

Usage Guidelines None

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 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** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface
rbridge-id	Specifies a switch by its RBridge identifier.
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. Refer to "Usage Guidelines" below.
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 Brocade VCS Fabric mode.
detail	Displays the IGMPv3 source information.

Defaults None

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.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples None

See Also None

show ip igmp interface vlan

Displays information related to VLANs in the IGMP protocol module.

Synopsis **show ip igmp interface vlan** *vlan_id*

Operands

vlan *vlan_id*	Specifies which VLAN interface to display the snooping configuration related information. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information related to VLANs in the IGMP protocol module.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples

```
switch# show ip igmp interface vlan 1
Interface Vlan 1
 IGMP Snooping disabled
 IGMP Snooping fast-leave disabled
 IGMP Snooping querier disabled
 Number of router-ports: 0
```

See Also 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. Refer to "Usage Guidelines" below.

mrouter interface vlan *vlan_id*
Specifies which VLAN interface to display the snooping configuration related information. Refer to "Usage Guidelines" below.

Defaults None

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 On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To display IGMP snooping information for VLAN 5:

```
switch# show ip igmp snooping interface vlan 5
```

See Also None

show ip igmp statistics interface

Displays IGMP statistics.

Synopsis **show ip igmp statistics interface vlan** *vlan_id*

Operands

vlan *vlan_id*	Specifies which VLAN interface to display the snooping configuration related information. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display IGMP statistics for an interface VLAN.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples

```
switch# show ip igmp statistics interface vlan 1
IGMP packet statistics for all interfaces in Vlan 1:
IGMP Message type      Received        Sent        Rx-Errors
Membership Query              0           0                0
V1 Membership Report          0           0                0
V2 Membership Report          0           0                0
Group Leave                   0           0                0
V3 Membership Report          0           0                0

IGMP Error Statistics:
Unknown types            0
Bad Length               0
Bad Checksum             0
```

See Also None

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* | **tengigabitethernet** *rbridge-id/slot/port* |**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* |**vlan** *vlan_id*]

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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
fortygigabitethernet	Specifies a valid 40 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
vlan *vlan_id*	Specifies to display a the VLAN number. Refer to "Usage Guidelines" below.

Defaults None

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 The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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 1/0/0 unassigned      up                     up
TenGigabitEthernet 1/0/1 unassigned      up                     down
TenGigabitEthernet 1/0/2 unassigned      up                     up
TenGigabitEthernet 1/0/3 unassigned      up                     up
TenGigabitEthernet 1/0/4 unassigned      up                     down
TenGigabitEthernet 1/0/5 unassigned      up                     down
TenGigabitEthernet 1/0/6 unassigned      up                     down
TenGigabitEthernet 1/0/7 unassigned      up                     up
TenGigabitEthernet 1/0/8 unassigned      up                     up
TenGigabitEthernet 1/0/9 unassigned      up                     up
TenGigabitEthernet 1/0/10 unassigned      up                     down
TenGigabitEthernet 1/0/11 unassigned      up                     down
TenGigabitEthernet 1/0/12 unassigned      up                     up
TenGigabitEthernet 1/0/13 unassigned      up                     up
TenGigabitEthernet 1/0/14 unassigned      up                     down
TenGigabitEthernet 1/0/15 unassigned      up                     up
TenGigabitEthernet 1/0/16 unassigned      up                     down
TenGigabitEthernet 1/0/17 unassigned      up                     up
TenGigabitEthernet 1/0/18 unassigned      up                     down
TenGigabitEthernet 1/0/19 unassigned      up                     up
TenGigabitEthernet 1/0/20 unassigned      up                     up
TenGigabitEthernet 1/0/21 unassigned      up                     up
TenGigabitEthernet 1/0/22 unassigned      up                     up
TenGigabitEthernet 1/0/23 unassigned      up                     up
Vlan 1                    unassigned      administratively down  down
Vlan 100                  unassigned      administratively down  down
Vlan 200                  unassigned      administratively down  down
```

To display the IP interface status of a 1 Gbps port on a Brocade 6710:

```
switch# show ip interface gigabitethernet 1/0/1
GigabitEthernet 1/0/1 is up protocol is up
IP unassigned
Proxy Arp is not Enabled
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switchin gis enabled
```

See Also show interface

show ip ospf

Displays OSPF state.

Synopsis **show ip ospf**

Operands This command has no operands.

Default None

Command Modes Privileged EXEC mode.

Description Displays OSPF state.

Usage Guidelines None

Examples

```
Switch(conf-if-vl-10)#show ip ospf
OSPF Version                    Version 2
Router Id                       1.1.1.1
ASBR Status                     No
ABR Status                      Yes        (1)
Redistribute Ext Routes from
Initial SPF schedule delay      0          (msecs)
Minimum hold time for SPFs      0          (msecs)
Maximum hold time for SPFs      0          (msecs)
External LSA Counter            0
External LSA Checksum Sum       00000000
Originate New LSA Counter       79
Rx New LSA Counter              74
External LSA Limit              14447047
Database Overflow Interval      0
Database Overflow State :       NOT OVERFLOWED
RFC 1583 Compatibility :        Disabled
NSSA Translator:                Enabled
Graceful Restart:               Disabled,   timer 120
Graceful Restart Helper:        Enabled
```

See Also None

show ip ospf area

Displays the OSPF area table.

Synopsis **show ip ospf area** {*A.B.C.D* | *decimal*} **database link-state** [**advertise** *index*] [**asbr** [{*asbrid* | **adv-router** *rid* }]] | [**extensive**] [**link-state-id** *lid*] [**network** [{*netid* | **adv-router** *rid* }]] [**nssa** [{*nsaaid* | **adv-router** *rid*}]] [**router** [{*routerid* | **adv-router** *rid*}]] [**router-id** *rid*] [**self-originate**] [**sequence-number** *num*] [**summary** [{*lid* | **adv-router** *rid*}]]

Operands

A.B.C.D	Area address in dotted decimal format.
decimal	Area address in decimal format. Range is 0 to 2147483647.
advertise *index*	Shows link state by Link State Advertisement (LSA) index.
asbr	Shows link state for all autonomous system boundary router (ASBR) links.
asbrid	Shows the state of a single ASBR link that you specify.
adv-router *rid*	Shows link state by the advertising router that you specify.
extensive	Shows detailed information for all entries in the OSPF database.
link-state-id *lid*	Shows link state by link-state ID.
network	Shows link state by network link.
netid	Shows link state of a particular network link that you specify.
adv-router *rid*	Shows link state by the advertising router that you specify.
nssa	Shows link state by not-so-stubby area (NSSA).
nsaaid	Shows link state of a particular NSAA area that you specify.
adv-router *rid*	Shows link state by the advertising router that you specify.
router	Shows link state by router link.
routerid	Shows link state of a particular router link that you specify.
adv-router *rid*	Shows link state by the advertising router that you specify.
router-id *rid*	Shows link-state by advertising router that you specify.
self-originate	Shows self-originated link states.
sequence-number *num*	Shows link-state by sequence number that you specify.
Summary	Shows link state summary. Can specify link-state ID or advertising router ID.

Default None

Command Modes Privileged EXEC mode.

Description Displays the OSPF area address table in the format you have chosen.

Usage Guidelines None

Examples

```
switch#show ip ospf area
Number of Areas is 4
```

```
Indx Area            Type   Cost       SPFR       ABR   ASBR  LSA
Chksum(Hex)
1    10.0.0.0        normal 0          4          0     0     0     00000000
2    11.0.0.0        normal 0          3          0     0     0     00000000
3    4               nssa   120        0          0     0     0     00000000
4    6               stub   110        0          0     0     0     00000000
```

See Also None

show ip ospf border-routers

Displays information about border routers and boundary routers.

Synopsis **show ip ospf border-routers** [*A.B.C.D*]

Operands

A.B.C.D	Specifies the router ID in dotted decimal format.

Default None

Command Modes Privileged EXEC mode.

Description Displays information about area border routers (ABRs) and autonomous system boundary routers (ASBRs). You can display information for all ABRs and ASBRs or for a specific router.

Examples To display information for all ABRs and ASBRs:

```
switch# show ip ospf border-routers
      router ID       router type next hop router outgoing interface Area
1     1.0.0.1         ABR         22.22.22.2      2/2                7
1     1.0.0.2         ABR         22.22.22.2      2/2                7
1     1.0.0.1         ASBR        22.22.22.2      2/2                7
1     1.0.0.2         ASBR        22.22.22.2      2/2                7
```

See Also None

show ip ospf config

Displays OSPF configuration.

Synopsis **show ip ospf config**

Operands This command contains no operands.

Default None

Command Modes Privileged EXEC mode.

Examples

```
switch(conf-if-vl-10)# show ip ospf config
Router OSPF: Enabled

Redistribution: Disabled
Default OSPF Metric: 10
OSPF Auto-cost Reference Bandwidth: Disabled
OSPF Redistribution Metric: Type2

OSPF External LSA Limit: 14447047

OSPF Database Overflow Interval: 0

RFC 1583 Compatibility: Enabled

Router id: 2.2.2.1
Interface State Change Trap:                       Disabled
Virtual Interface State Change Trap:               Disabled
Neighbor State Change Trap:                        Disabled
Virtual Neighbor State Change Trap:                Disabled
Interface Configuration Error Trap:                Disabled
Virtual Interface Configuration Error Trap:        Disabled
Interface Authentication Failure Trap:             Disabled
Virtual Interface Authentication Failure Trap:     Disabled
Interface Receive Bad Packet Trap:                 Disabled
Virtual Interface Receive Bad Packet Trap:         Disabled
Interface Retransmit Packet Trap:                  Disabled
Virtual Interface Retransmit Packet Trap:          Disabled
Originate LSA Trap:                                Disabled
Originate MaxAge LSA Trap:                         Disabled
Link State Database Overflow Trap:                 Disabled
Link State Database Approaching Overflow Trap:     Disabled

OSPF Area currently defined:
Area-ID          Area-Type Cost
4                nssa      120
6                stub      110
7                normal    0
0                normal    0



OSPF Virtual Link Interfaces currently defined:
```

```
area 7              virtual-link 192.0.0.1               dead-int 40
area 7              virtual-link 192.0.0.1
hello-int                    10            area 7
virtual-link 192.0.0.1      retransmit-int 5,   area 7
virtual-link 1.1.1.1
ip ospf md5-authentication-key ********
ip ospf md5-authentication-key-id 32
ip ospf auth-change-wait-time 300


OSPF Redistribution currently defined:
 deny redistribute 9 all
```

See Also None

show ip ospf database

Shows database information.

Synopsis **show ip ospf database database-summary**

show ip ospf database external-link-state [**advertise** *index*] [**extensive**] [**link-state-id** *lid*] [**router-id** *routerid*] [**sequence-number** *num*]

show ip ospf database link-state [**advertise** *index*] [**asbr** [{*asbrid* | **adv-router** *rid* }]] | [**extensive**] [**link-state-id** *lid*] [**network** [{ *netid* | **adv-router** *rid* }]] [**nssa** [{*nsaaid* | **adv-router** *rid*}]] [**router** [{*routerid* | **adv-router** *rid*}]] [**router-id** *rid*] [**self-originate**] [**sequence-number** *num*] [**summary** [{ *lid* | **adv-router** *rid*}]

Operands

database-summary	Shows how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.
external-link-state	Shows information by external link state, based on the following options:
advertise *index*	Shows the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's External LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.
extensive	Shows LSAs in decrypt format. Do not use this option in combination with other display options because the entire database is displayed.
link-state-id *lid*	Shows external LSAs for the LSA source that you specify.
router-id *routerid*	Shows external LSAs for the advertising router that you specify.
sequence-number *num*	Shows the External LSA entries for the hexadecimal LSA sequence number that you specify.
link-state	Shows link state, based on the following options:
advertise *index*	Shows the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's external-LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.
asbr	Shows autonomous system boundary router (ASBR) LSAs.
extensive	Shows LSAs in decrypt format. Do not use this option in combination with other display options because the entire database is displayed.
link-state-id *lid*	Shows LSAs for the LSA source that you specify.
network	Shows either all network LSAs or the LSAs for a network that you specify.
nssa	Shows either all NSSA LSAs or the LSAs for a not-so-stubby area (NSSA) that you specify.
router	Shows LSAs by router link.
router-id *routerid*	Shows LSAs for the advertising router that you specify.
self-originate	Shows self-originated LSAs.

sequence-number
Shows the LSA entries for the hexadecimal LSA sequence number that you specify.

summary Shows summary information. Can specify link-state ID or advertising router ID.

Default None

Command Modes Privileged EXEC mode.

Description Displays debug information based on the options you enable.

Examples

```
switch# show ip ospf database
Link States

Index Area ID         Type LS ID           Adv Rtr         Seq(Hex)
Age  Cksum
1     6               Summ 0.0.0.0         22.22.22.1      80000002
1    0xbfec
2     7               Rtr  22.22.22.1      22.22.22.1      80000002
6    0xb8cc
3     0               Summ 22.22.22.0      22.22.22.1      80000001
6    0x4294

switch#sh ip ospf database

Link States

Index Area ID         Type LS ID           Adv Rtr         Seq(Hex)
Age  Cksum
1     6               Summ 0.0.0.0         22.22.22.1      80000002 52
0xbfec
2     7               Rtr  22.22.22.1      22.22.22.1      80000003
7    0xda66
3     7               Rtr  1.0.0.2         1.0.0.2         80000001 1248
0xee99
4     7               Rtr  192.0.0.1       192.0.0.1       80000006
8    0x9c80
5     7               Rtr  1.0.0.1         1.0.0.1         80000001 1248
0xfe8b
6     7               Net  22.22.22.1      22.22.22.1      80000002
7    0xb419
7     7               Summ 1.0.2.0         1.0.0.1         80000001 1248
0x4314
8     7               Summ 1.0.0.0         1.0.0.1         80000001 1248
0x59ff
9     7               Summ 1.0.3.0         1.0.0.2         80000001 1248
0x3223
10    7               Summ 1.0.1.0         1.0.0.1         80000001 1248
0x4e0a
11    7               Summ 1.0.4.0         1.0.0.2         80000001 1248
0x272d
12    0               Summ 22.22.22.0      22.22.22.1      80000001 57
0x4294
13    0               ASBR 1.0.0.2         22.22.22.1      80000001
7    0x38db
```

```
14    0               ASBR 1.0.0.1         22.22.22.1      80000001
7    0x42d2

Type-5 AS External Link States

Index Age  LS ID           Router          Netmask  Metric   Flag Fwd Address
1     1248 1.0.5.0         1.0.0.1         ffffff00 00000001 0000 0.0.0.0
2     1248 1.0.8.0         1.0.0.2         ffffff00 00000001 0000 0.0.0.0
3     1248 1.0.6.0         1.0.0.1         ffffff00 00000001 0000 0.0.0.0
4     1248 1.0.7.0         1.0.0.2         ffffff00 00000001 0000 0.0.0.0
```

See Also None

show ip ospf interface

Displays interface information.

Synopsis **show ip ospf interface** [{*A.B.C.D* | **FortyGigabitEthernet** *rbridge-id/slot/port* [**brief**]| **GigabitEthernet** *rbridge-id/slot/port* [**brief**] | **Port-channel** *number* [**brief**] | **TenGigabitEthernet** *rbridge-id/slot/port* [**brief**] |**ve** *vlan #* [**brief**] } [**brief**]]

Operands

A.B.C.D	Specifies interface IP address in dotted decimal format.
FortyGigabitEthernet *rbridge-id/slot/port*	Specifies a valid 40-Gbps port interface.
rbridge-id	Specifies the ID of the routing bridge. This operand is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
brief	Displays brief summary information about the specified port.
GigabitEthernet *rbridge-id/slot/port*	Specifies a valid 1-Gbps Ethernet interface
rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
brief	Displays brief summary information about the specified port.
Port-channel *number*	Specifies the port-channel number. The range of valid values is 1 through 6144.
brief	Displays brief summary information about the specified port channel.
tenGigabitEthernet *rbridge-id/slot/port*	Specifies a valid 10-Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
brief	Displays brief summary information about the specified port.
ve *vlan#*	Specifies the vlan number.
brief	Displays brief summary information about the specified vlan.
brief	Displays brief summary about all enabled interfaces.

Default None

Command Modes Privileged EXEC mode.

Description Displays information about all or specific OSPF-enabled interfaces.

Examples To display information about all enabled interfaces:

```
switch# show ip ospf interface
eth 2/2, OSPF enabled
     IP Address 22.22.22.1, Area 7
     Database Filter: Not Configured
     OSPF state DR, Pri 1, Cost 1, Options 2, Type broadcast Events 5
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 2.2.2.1           Interface Address 22.22.22.1
     BDR: Router ID 0.0.0.0           Interface Address 0.0.0.0
     Neighbor Count = 1, Adjacent Neighbor Count= 1
     Neighbor:         22.22.22.2
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id None, Auth-change-wait-time 300
```

See Also None

show ip ospf neighbor

Displays neighbor information.

Synopsis **show ip ospf neighbor** [{**extensive** | **FortyGigabitEthernet** *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **Port-channel** *number* | **router-id** *A.B.C.D* | **TenGigabitEthernet** *rbridge-id/slot/port* | **ve** *vlan#* }]

Operands

extensive Shows detailed information about all neighbors.

FortyGigabitEthernet *rbridge-id/slot/port*
Show neighbor information for the specified, valid 40-Gbps port interface.

- *rbridge-id* Specifies the ID of the routing bridge. This operand is not valid in standalone mode.
- *slot* Specifies a valid slot number.
- *port* Specifies a valid port number.

GigabitEthernet *rbridge-id/slot/port*
Show neighbor information for the specified, valid 1-Gbps Ethernet interface

- *rbridge-id* Specifies the ID of the routing bridge.
- *slot* Specifies a valid slot number.
- *port* Specifies a valid port number.

Port-channel *number*
Show neighbor information for the specified, valid port-channel number. The range of valid values is 1 through 6144.

router-id *A.B.C.D* Show neighbor information for the specified router ID (in dotted decimal format).

tenGigabitEthernet *rbridge-id/slot/port*
Show neighbor information for the specified, valid 10-Gbps Ethernet interface.

- *rbridge-id* Specifies the ID of the routing bridge.
- *slot* Specifies a valid slot number.
- *port* Specifies a valid port number.

ve *vlan#* Show neighbor information for the specified vlan number.

Default None

Command Modes Privileged EXEC mode.

Description Displays information about OSPF neighbors.

Examples To show information about all OSPF neighbors:

```
switch# show ip ospf neighbor
Number of Neighbors is 2, in FULL state 1

Port  Address         Pri State      Neigh Address   Neigh ID        Ev Opt
Cnt
2/2   22.22.22.1      0   FULL/OTHER 22.22.22.2      192.0.0.1       5  2   0
```

See Also None

show ip ospf routes

Displays routes.

Synopsis **show ip ospf routes** [*A.B.C.D*]

Operands *A.B.C.D* Specifies a destination IP address in dotted decimal format.

Default None

Command Modes Privileged EXEC mode.

Description Displays routes that OSPF calculated. You can display all routes or you can display information about a specific route.

Examples To display all OSPF-calculated routes:

```
switch# show ip ospf routes
OSPF Regular Routes 2:

      Destination     Mask            Path_Cost Type2_Cost Path_Type
      2.2.2.0         255.255.255.0   1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      2.2.2.1         2.2.2.1         Network   Valid      0          4000*
      Paths Out_Port        Next_Hop        Type      State
      1     eth 1/2         0.0.0.0         OSPF      00 00

      Destination     Mask            Path_Cost Type2_Cost Path_Type
      22.22.22.0      255.255.255.0   1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      2.2.2.1         22.22.22.1      Network   Valid      0          4000*
      Paths Out_Port        Next_Hop        Type      State
      1     eth 2/2         0.0.0.0         OSPF      00 00
```

See Also None

show ip ospf summary

Displays summary information for all OSPF instances.

Synopsis **show ip ospf summary**

Operands This command has no operands.

Default None

Command Modes Privileged EXEC mode.

Examples

```
switch# show ip ospf summary
Total number of OSPF instances: 1

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2


telnet@NetIron MLX-4 Router(config-ospf-router)#show ip ospf border-routers
      router ID       router type next hop router outgoing interface Area
1     1.0.0.1         ABR         22.22.22.2      2/2                7
1     1.0.0.2         ABR         22.22.22.2      2/2                7
1     1.0.0.1         ASBR        22.22.22.2      2/2                7
1     1.0.0.2         ASBR        22.22.22.2      2/2                7
```

See Also None

show ip ospf traffic

Displays OSPF traffic details.

Synopsis **show ip ospf traffic** [{**FortyGigabitEthernet** *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **Port-channel** *number* | **TenGigabitEthernet** *rbridge-id/slot/port* | **ve** *vlan#* }]

Operands

FortyGigabitEthernet *rbridge-id/slot/port*
Show traffic information for the specified, valid 40-Gbps port interface.

rbridge-id	Specifies the ID of the routing bridge. This operand is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

GigabitEthernet *rbridge-id/slot/port*
Show traffic information for the specified, valid 1-Gbps Ethernet interface

rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Port-channel *number*
Show traffic information for the specified, valid port-channel number. The range of valid values is 1 through 6144.

tenGigabitEthernet *rbridge-id/slot/port*
Show traffic information for the specified, valid 10-Gbps Ethernet interface.

rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

ve *vlan#* Show traffic information for the specified vlan number.

Default None

Command Modes Privileged EXEC mode.

Description Displays details of OSPF traffic sent and received. You can display all traffic or specify a particular interface.

Examples To show all OSPF traffic:

```
switch# show ip ospf traffic
Packets Received         Packets Sent
Hello                          10                    10
Database                       90                    89
LSA Req                        12                    11
LSA Upd                        12                    12
LSA Ack                        12                    12
No Packet Errors!
```

2 show ip ospf traffic

See Also None

show ip ospf virtual

Displays information about virtual links.

Synopsis **show ip ospf virtual** {**link** | **neighbor**} [*index*]

Operands

link *index*	Shows information about all virtual links or one virtual link that you specify.
neighbor *index*	Shows information about all virtual neighbors or one virtual neighbor that you specify.

Default None

Command Modes Privileged EXEC mode.

Description Displays information about virtual links and virtual neighbors over virtual links. You can show information about all virtual links or virtual neighbors, or you can specify a specific virtual link or virtual neighbor.

Examples To show information about all virtual links:

```
switch# show ip ospf virtual link
Indx Transit Area     Router ID        Transit(sec) Retrans(sec) Hello(sec)
1    7                192.0.0.1        1            5            10
     Dead(sec)        events           state        Authentication-Key
     40               0                down         None
     MD5 Authentication-Key:       None
     MD5 Authentication-Key-Id:    None
     MD5 Authentication-Key-Activation-Wait-Time:      300
```

To show information about all virtual neighbors:

```
switch# show ip ospf virtual neighbor
Indx Transit Area     Router ID        Transit(sec) Retrans(sec) Hello(sec)
1    7                192.0.0.1        1            5            10
     Dead(sec)        events           state        Authentication-Key
     40               0                down         None
     MD5 Authentication-Key:       None
     MD5 Authentication-Key-Id:    None
     MD5 Authentication-Key-Activation-Wait-Time:      300
```

See Also None

show ip route

Shows route information.

Synopsis

show ip route

show ip route *A.B.C.D/M* [{**debug** | **detail** | **longer**}]

show ip route [**all**] [**connected**] [**ospf**] [**slot** *line_card_number*] [**static**] [**summary**]

show ip route nexthop [*nexthopID* [**ref-routes**]]

Operands

A.B.C.D/M	Specifies the IPv4 address/length to show information for a specific route.
debug	Shows debug information.
detail	Shows more-specific routes with the same specified prefix.
longer	
all	Shows information for all configured ip routes.
connected	Shows directly connected routes, such as local L3 interfaces.
ospf	Shows routes learned from the Open Shortest Path First (OSPF) protocol.
slot *line_card_number*	Shows information for routes with the provided line card number.
static	Shows information about the configured static routes.
summary	Shows summary information for all routes.
nexthop	Shows information about the configured next hop.
nexthopID	Range is 0 to 65535.
ref-routes	Shows all routes that point to the specified *nexthopID*.

Default None

Command Modes Privileged EXEC mode.

Description Displays information about the IP routes in IP route management.

Usage Guidelines None

Examples

```
switch# show ip route
Total number of IP routes: 7
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       1.1.1.0/24         DIRECT          Te 2/1      0/0           D    1m57s
2       1.1.2.0/24         DIRECT          Te 2/2      0/0           D    0m6s
3       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    1m32s
4       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    1m16s
5       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    1m13s
6       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    0m57s
7       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    0m5s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    0m5s
```

```
switch# show ip route connected
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       1.1.1.0/24         DIRECT          Te 2/1      0/0           D    4m33s
2       1.1.2.0/24         DIRECT          Te 2/2      0/0           D    2m42s
sw0(config)# do show ip route summary
IP Routing Table - 7 entries:
  2 connected, 5 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS
  Number of prefixes:
  /24: 7
Nexthop Table Entry - 4 entries
sw0(config)# do show ip route static
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    4m27s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    4m11s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    4m8s
4       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    3m52s
5       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    3m0s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    3m0s


switch# show ip route nexthop
Total number of IP nexthop entries: 4; Forwarding Use: 4
       NextHopIp        Port            RefCount      ID          Age
1      1.1.1.2          Te 2/1          3/3           2147549184 277
2      0.0.0.0          Te 2/2          1/1           2147484008 191
3      0.0.0.0          Te 2/1          2/2           2147484009 302
4      1.1.1.2          Te 2/1          1/1           2147549185 190
       1.1.2.2          Te 2/2


switch# show ip route nexthop 2147549184
       NextHopIp        Port            RefCount      ID          Age
1      1.1.1.2          Te 2/1          3/3           2147549184 288


switch# show ip route nexthop 2147549184 ref-routes
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m10s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    4m54s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1


switch# show ip route 100.1.1.1
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
```

```
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
4       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m37s
sw0(config)# do show ip route 100.1.1.0/24
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
5       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m47s

sw0(config)# do show ip route 100.1.1.1 detail
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
6       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    6m5s
        Nexthop Entry ID:2147549184, Paths: 1, Ref_Count:3/3

switch# show ip route 100.0.0.0/8 longer
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    14m37s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    14m21s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    14m18s
4       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    14m2s
5       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    13m10s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    13m10s
```

show lacp counters

Displays the LACP statistics.

Synopsis **show lacp counters** [*port-channel-id*]

Operands *port-channel-id* The port channel ID. The range of valid values is from 1 through 6144.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the LACP statistics for each port-channel interface, or for all port-channel interfaces.

Usage Guidelines None

Examples None

See Also None

show lacp sys-id

Displays the Link Aggregation Control Protocol (LACP) system ID and priority information.

Synopsis **show lacp sys-id**

Operands None

Defaults None

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 8000,00-05-1e-76-1a-a6
```

See Also None

show license

Displays license information.

Synopsis **show license** [**rbridge-id** *ID* | **all**]

Operands

rbidge-id *ID*	Executes the command on the remote switch specified by the RBridge ID.
all	Executes the command on all switches in the fabric.

Defaults By default, this command displays the licenses installed 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 Brocade VCS Fabric cluster. The command output includes the RBridge ID, license description, expiration if applicable, and the feature name. A string of “x” characters is displayed for the license key

If no operand is specified, the command executes on the local switch.

Usage Guidelines In the Network OS v3.0.0 release this command displays only the licenses installed on the local RBridge.

Examples To display license information on a Brocade VDX 6720-60 switch:

```
switch# show license
Rbridge-Id: 2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    FCoE Base license
    Feature name:FCOE_BASE
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    First Ports on Demand license - additional 10 port upgrade license
    Feature name:PORTS_ON_DEMAND_1
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    Second Ports on Demand license - additional 10 port upgrade license
    Feature name:PORTS_ON_DEMAND_2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    VCS Fabric license
    Feature name:VCS_Fabric
```

To display a Brocade VDX 8770 licensed for Advanced Services. This configuration enables the use of Layer 3, FCoE, and VCS features.

```
switch# show license
rbridge-id: 60
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       Advanced Services license
       Feature name:ADVANCED_SERVICES
```

See Also license add, license remove, show license id

show license id

Displays the routing bridge License ID.

Synopsis **show license id** [**rbridge-id** *ID* | **all**]

Operands

license-id *ID*	Executes the command on the remote switch specified by the RBridge ID.
all	Executes the command on all switches in the fabric.

Defaults By default, this command displays the license ID installed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the routing bridge license ID (WWN) for the specified switch. You need the routing bridge license ID when you add a license.

If no operand is specified, the command is executed on the local switch.

Usage Guidelines In the Network OS v3.0.0 release this command is supported only on the local RBridge.

Examples To display the license ID for the local switch:

```
switch# show license id
Rbridge-Id               LicenseId
=======================================
2               10:00:00:05:1E:00:4C:80
```

See Also license add, license remove, show license

show linecard

Displays information about the interface modules (line cards) present in the chassis.

Synopsis **show linecard**

Operands *None*

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the interface modules present in a modular switch. The output includes the following information:

Slot	Displays the slot number. Slots for interface modules are L1 through L4 on the Brocade VDX 8770-4, and L1 through L8 on the Brocade VDX 8770-8.
Type	Displays the interface module type. Valid types include the following
LC48X10G	48-port 10 GbE interface module (line card)
LC48X1G	48-port 1 GbE interface module (line card)
LC12X40G	12-port 40 GbE interface module
Description	Module description
ID	IDs for interface modules include the following:
114	48-port 10GbE interface module
127	12-port 40 GbE interface module
131	48-port 1 GbE interface module
Status	Displays the status of the module as one of the following:
VACANT	The slot is empty.
POWERED-OF	The module is present in the slot but is powered off.
POWERING UP	The module is present and powering on.
LOADING	The module is present, powered on, and loading the initial configuration.
DIAG RUNNING POST1	The module is present, powered on, and running the POST (power-on self-test).
DIAG RUNNING POST2	The module is present, powered on, and running the reboot power on self tests.
INITIALIZING	The module is present, powered on, and initializing hardware components.
ENABLED	The module is on and fully enabled.
DISABLED	The module is powered on but disabled.
FAULTY	The module is faulty because an error was detected.
UNKNOWN	The module is inserted but its state cannot be determined.

Usage Guidelines None

Examples To display the interface modules present in a Brocade VDX 8770-4 chassis:

```
switch# show linecard
Slot  Type         Description                ID      Status
--------------------------------------------------------------------
 L1   LC48X10G     48-port 10GE card          114     ENABLED
 L2   LC48X10G     48-port 10GE card          114     ENABLED
 L3                                           VACANT
 L4   LC48X1G      48-port 1GE card           131     ENABLED
```

See Also linecard, show sfm, show slots

show lldp interface

Displays the LLDP status on the specified interface.

Synopsis **show lldp interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the LLDP status on the specified interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display all the LLDP interface information for a selected interface:

```
switch# show lldp interface tengigabitethernet 1/0/0
LLDP information for Te 1/0/0
  State:                   Enabled
  Mode:                    Receive/Transmit
  Advertise Transmitted:   30 seconds
  Hold time for advertise: 120 seconds
  Re-init Delay Timer:     2 seconds
  Tx Delay Timer:          1 seconds
  DCBX Version :           CEE
  Auto-Sense :             Yes
  Transmit TLVs:           Chassis ID              Port ID
                           TTL                     IEEE DCBX
                           DCBX FCoE App           DCBX FCoE Logical Link
                           Link Prim               Brocade Link
  DCBX FCoE Priority Bits: 0x8
```

See Also None

show lldp neighbors

Displays LLDP information for all neighboring devices on the specified interface.

Synopsis **show lldp neighbors** [**interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*} **detail**]

Operands

interface		Use this keyword to specify an Ethernet interface using the following operands:
tengigabitethernet		Specifies a valid 10 Gbps Ethernet interface.
	rbridge-id	Specifies a switch by its RBridge identifier.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.
gigabitethernet		Specifies a valid 1 Gbps Ethernet interface.
	rbridge-id	Specifies a switch by its RBridge identifier.
	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 None

Command Modes Privileged EXEC mode

Description Use this command to display LLDP information for all neighboring devices on the specified interface.

If you do not use the **interface** operand, only the mandatory TLVs are displayed.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display detailed LLDP neighbor information on a specific interface:

```
switch# show lldp neighbors interface tengigabitethernet 3/0/8 detail

Neighbors for Interface Te 3/0/8

MANDATORY TLVs
===============
Local Interface: Te 0/8    Remote Interface: Te 3/0/8 (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 3/0/8
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
```

See Also None

show lldp statistics

Displays the LLDP statistics on all interfaces or a specified interface.

Synopsis **show lldp statistics** [**interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*}]

Operands

interface		Use this keyword to specify an Ethernet interface using the following operands:
	tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
	rbridge-id	Specifies a switch by its RBridge identifier.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
	rbridge-id	Specifies a switch by its RBridge identifier.
	slot	Specifies a valid slot number.
	port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display LLDP statistics on all interfaces or a specified interface.

If you do not specify an interface, this command displays the LLDP statistics for all interfaces.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display LLDP statistics on the specified interface:

```
switch# show lldp statistics interface tengigabitethernet 5/0/8
LLDP Interface statistics for Te 5/0/8
Frames transmitted: 555
Frames Aged out:    0
Frames Discarded:   0
Frames with Error:  0
Frames Recieved:    554
TLVs discarded:     0
TLVs unrecognized:  0
```

See Also None

show logging auditlog

Displays the internal audit log buffer of the switch.

Synopsis **show logging auditlog [reverse] [rbridge-id** *rbridge-id***]**

Operands

reverse	Displays the audit log in reverse order.
rbridge-id	Executes the command on the specified switch.
rbridge-id	Specifies the unique identifier for the switch.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the audit log messages stored in the system.

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

Examples To display the audit log messages stored in the internal buffer:

```
switch# show logging auditlog
0 AUDIT,2012/04/13-02:35:59 (GMT), [DCM-2002], INFO, DCMCFG,
admin/admin/10.72.16.41/ssh/cli,, chassis, Event: noscli exit, Status:
success, Info: Successful logout by user [admin].

1 AUDIT,2012/04/13-02:43:23 (GMT), [DCM-2001], INFO, DCMCFG,
admin/admin/10.72.16.41/ssh/cli,, chassis, Event: noscli start, Status:
success, Info: Successful login attempt through ssh from 10.72.16.41.
```

See Also clear logging raslog, clear logging auditlog, logging auditlog class

show logging raslog

Displays the internal RASlog buffer of the switch.

Synopsis **show logging raslog [attribute** *attribute*] [**blade** *blade*] [**count** *count*] [**message-type** *type*] [**reverse**][**severity** *severity*][**rbridge-id** *rbridge-id*]

Operands

attribute *attribute*	Filters output by message attribute. Valid attributes include FFDC and VCS.
blade *blade*	Displays for the specified blade only. Valid values for blade include MM1, MM2, and LC[1-8].
count *count*	Specify the number of messages to display.
message-type *type*	Filters the output by message type. Valid message types include DCE or SYSTEM.
severity *severity*	Filters the output by message severity. Valid severity levels include the following: critical, error, info, and warning.
reverse	Displays the messages in reverse order.
rbridge-id *rbridge-id*	Executes the command on the specified switch.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the RASlog messages stored in the system. Use the filters to customize the output.

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

The RASlog messages contain the module name, error code, and message details.

Examples To display all RASlog messages stored in the system:

```
switch# show logging raslog
NOS: 3.0.0
2012/05/25-17:37:15, [LOG-1003], 1, M1, INFO, VDX8770-4, SYSTEM error log has
been cleared

2012/05/25-17:38:32, [SEC-1203], 3, M1, INFO, sw0, Login information: Login
successful via TELNET/SSH/RSH. IP Addr: 10.24.65.24

2012/05/25-17:42:54, [SEC-1203], 4, M1, INFO, sw0, Login information: Login
successful via TELNET/SSH/RSH. IP Addr: 10.24.65.24

2012/05/25-17:43:12, [IPAD-1002], 5, M1, INFO, VDX8770-4, Switch name has
been successfully changed to dutA1-sw0.

2012/05/25-17:51:42, [FW-1439], 180, M1, WARNING, dutA1-sw0, Switch status
change contributing factor Switch offline.
(output truncated)
```

To display all RASlog messages for an interface module:

```
switch# show logging raslog blade LC2
```

```
NOS: 3.0.0
2012/05/28-12:07:41, [HASM-1004], 822, L2, INFO, VDX8770-4, Processor
rebooted - Reset

2012/05/28-12:07:41, [HASM-1104], 823, L2, INFO, VDX8770-4, Heartbeat to M1
up

2012/05/28-12:07:48, [HASM-1108], 830, L2, INFO, VDX8770-4, All service
instances become active.

2012/05/29-13:32:50, [HASM-1004], 2721, L2, INFO, VDX8770-4, Processor
rebooted - Reset
```

To display warning messages only on the standby management module:

```
switch# show logging raslog blade MM1 severity warning
NOS: 3.0.0
2012/03/09-15:20:55, [FW-1042], 26, M1, WARNING, dutA1-sw0, Sfp TX power for
port 1/2/9, is below low boundary(High=1999, Low=125). Current value is 17 uW.

2012/03/09-15:20:55, [FW-1046], 27, M1, WARNING, dutA1-sw0, Sfp Current for
port 1/2/9, is below low boundary(High=10, Low=3). Current value is 0 mA.

2012/03/09-15:20:55, [FW-1042], 28, M1, WARNING, dutA1-sw0, Sfp TX power for
port 1/2/17, is below low boundary(High=1999, Low=125). Current value is 18
uW.
(output truncated)
```

To display only the FFDC messages:

```
switch# show logging raslog attribute FFDC rbridge-id 1
NOS: 3.0.0
1970/01/01-00:09:43, [HASM-1200], 106, MM1 | FFDC, WARNING, chassis, Detected
termination of process Dcmd.Linux.powe:1660
To display only 3 entries (unfiltered) in reverse order:
switch#show logging raslog attribute FFDC rbridge-id 1
NOS: 3.0.0
1970/01/01-00:06:18, [FW-1433], 497, MM1, WARNING, sw0, Switch status change
contributing factor CP: CP non-redundant (Slot2/CP1) faulty.

1970/01/01-00:06:18, [FW-1431], 496, MM1, WARNING, sw0, Switch status change
contributing factor Fan: 2 bad.

1970/01/01-00:06:18, [FW-1428], 495, MM1, WARNING, sw0, Switch status change
contributing factor Power supply: 2 absent.
```

See Also clear logging raslog, logging raslog console

show mac-address-table

Displays forwarding information for all MAC addresses, for a specific dynamic or static MAC address, for all dynamic MAC addresses, for all static MAC addresses, for a specific interface, for a specific VLAN, or for MAC addresses associated with port profiles.

Synopsis **show mac-address-table** [**address** *mac-addr* | **aging-time** | **count** | **dynamic** | **interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*} | **linecard interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*} | **static** | **vlan** *vlan_id* | **port-profile** [**address mac-addr** | **count** | **dynamic** | **static** | **vlan** *vlan-id*]]

Operands

address *mac-address*
Displays forwarding information for 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.
  - *rbridge-id* Specifies a switch by its RBridge identifier.
  - *slot* Specifies a valid slot number.
  - *port* Specifies a valid port number.
- **gigabitethernet**
  Specifies a valid 1Gbps Ethernet interface.
  - *rbridge-id* Specifies a switch by its RBridge identifier.
  - *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 Displays the forwarding information for a linecard interface.

- **tengigabitethernet**
  Specifies a valid 10 Gbps Ethernet linecard interface.
  - *rbridge-id* Specifies a switch by its RBridge identifier.
  - *slot* Specifies a valid slot number.
  - *port* Specifies a valid port number.
- **gigabitethernet** Specifies a valid 1 Gbps Ethernet linecard interface.
  - *rbridge-id* Specifies a switch by its RBridge identifier.
  - *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. Refer to "Usage Guidelines" below.
port-profile	Displays MAC addresses associated with port profiles..
address *mac-address*	Specifies a 48-bit MAC address. The valid format is H.H.H.
count	Displays the count of forwarding entries associated with port profiles.
dynamic	Displays dynamic MAC addresses associated with port profiles.
static	Displays static MAC addresses associated with port profiles.
vlan *vlan-id*	Displays MAC addresses associated with port profiles and the specified VLAN.

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 The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

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
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 MAC addresses   : 2
```

See Also None

show media

Displays the SFP information for all the interfaces present on a switch.

Synopsis **show media**

Operands None

Defaults None

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 None

Examples To display all SFP information:

```
switch# show media interface tengigabitethernet 0/1
Interface TenGigabitEthernet 0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver    0000000000000010 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)
  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         0
  BR Min         0
  Serial No      AAA108454100431
  Date Code      081108
  Temperature    44 Centigrade
  Voltage        3246.8  (Volts)
  Current        0.002  (mAmps)
  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** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **fibrechannel** *rbridge-id/slot/port*]

Operands

tengigabitethernet	Specifies a valid external 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid external 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
fibrechannel	Specifies a valid external 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a summary of the SFP information for the specified interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

The **fibrechannel** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6730.

Examples To display SPF information for a 1 Gbps Ethernet interface:

```
switch# show media interface Gigabitethernet 1/0/1
  Interface       GigabitEthernet 0/1
  Identifier      2    On-board
  Connector       34   CAT-5 copper cable
  Transceiver     1000 BASE-T Gigabit Ethernet
  Name            cu
  Encoding        5    IEEE 802.3ab
  Length          max 100 m
  Copper Speed    1GB/s Fixed
  Copper Duplex   Full Duplex
  Sync status     Valid/No
  Vendor Name     Broadcom
  Vendor OUI      00:1B:E9
  Vendor model    02:0F
  Vendor Rev      01
  Options         001a Remote fault/Jabber detect/copper link up
```

```
    Temperature threshold/val    55 Centigrade
    Voltage threshold/val        3289.9  (mVolts)
```

To display SFP information for a 10 Gbps Ethernet interface:

```
switch#show media interface tengigabitethernet 5/0/1
Interface TenGigabitEthernet 5/0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver    0000000000000010 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)
  Length 62.5u   3   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1E
  Vendor PN      57-0000075-01
  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)
  Current        0.002  (mAmps)
  TX Power       0.1  (uWatts)
  RX Power       0.1  (uWatts)
```

To display SFP information for a Fibre Channel interface:

```
switch# show media interface fibrechannel 66/0/1
  Interface         FibreChannel 66/0/1
  Identifier        3    SFP
  Connector         7    LC
  Transceiver       540c404040000000 200,400,800_MB/s M5,M6 sw Short_dist
  Encoding          1    8B10B
  Baud Rate         85   (units 100 megabaud)
  Length 9u         0    (units km)
  Length 9u         0    (units 100 meters)
  Length 50u        5    (units 10 meters)
  Length 62.5u      2    (units 10 meters)
  Length Cu         0    (units 1 meter)
  Vendor Name       BROCADE
  Vendor OUI        00:05:1e
  Vendor PN         57-1000012-01
  Vendor Rev        A
  Wavelength        850  (units nm)
  Options           003a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max            0
  BR Min            0
  Serial No         UAF110170000VP1
  Date Code         100422
  DD Type           0x68
  Enh Options       0xfa
  Status/Ctrl       0x82
```

```
  Alarm flags[0,1]  0x5, 0x40
  Warn Flags[0,1]   0x5, 0x40
                                                  Alarm                 Warn
                                           low        high       low        high
Temperature    28      Centigrade      -10         90         -5         85
Voltage        3331.4  mVolts          2900.0      3700.0     3000.0     3600.0
Current        0.310   mAmps           1.000       17.000     2.000      14.000
TX Power      -21.7    dBm (6.8   uW) 125.9  uW   631.0  uW  158.5  uW  562.3  uW
RX Power      -inf    dBm (0.0   uW) 10.0   uW   1258.9 uW  15.8   uW   1000.0 uW
```

See Also show media, show media linecard

show media linecard

Displays the SFP information for a specified interface module.

Synopsis **show media linecard** number

Operands *number* Numeric identifier for the interface module.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a summary of Small Form-Factor Pluggable (SFP) and Quad SFP media information for each interface on the specified module.

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

Examples To display the SFP media information for an LC48X10G interface module in slot 2:

```
switch# show media linecard 2
Interface      TenGigabitEthernet 1/2/1
  Identifier     3    SFP
  Connector      33   Copper Pigtail
  Transceiver           d580884104000002 10_GB/s TW Short_dist
  Name           cu
  Encoding       0
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     0   (units 10 meters)
  Length 62.5u   0   (units 10 meters)
  Length Cu      1   (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1e
  Vendor PN      58-1000026-01
  Vendor Rev     A
  Wavelength     3072(units nm)
  Options        0012
  BR Max         0
  BR Min         0
  Serial No      CAMB110100607EW
  Date Code      110111
  Optical Monitor No
  Temperature    N/A
  Voltage        N/A
  Current        N/A
  TX Power       N/A
  RX Power       N/A
(output truncated)
```

To display the SFQ+ media information for an LC12X40G interface module in slot 3:

```
switch# show media linecard 3
Interface      FortyGigabitEthernet 1/3/2
  Identifier     13   QSFP
  Connector      12
  Transceiver           0000000000000004 40_GB/s  Short_dist
  Name           sw
```

```
Encoding       5    IEEE 802.3ab
Baud Rate      103 (units 100 megabaud)
Length 9u      0   (units km)
Length 9u      50  (units 100 meters)
Length 50u     0   (units 10 meters)
Length 62.5u   0   (units 10 meters)
Length Cu      0   (units 1 meter)
Vendor Name    5ROCADE
Vendor OUI     00:05:1e
Vendor PN      57-1000128-01
Vendor Rev     A
Wavelength     17000(units nm)
Options        0000
BR Max         15
BR Min         222
Serial No      LTA111421000923
Date Code      111022
Optical Monitor yes
Temperature    31 Centigrade
Voltage        3313.2  (mVolts)
Current        7.204  (mAmps)
TX Power       N/A
RX Power       0.0  (uWatts)
```

See Also linecard, show slots

show mm

Displays information about the management modules present in the chassis.

Synopsis **show mm**

Operands *None*

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the management modules present in a modular switch. The output includes the following information:

Slot	Displays the slot number. Slots for management modules are M1 and M2.
Type	Displays the interface module type. The management module type is MM.
Description	Module description
ID	Displays the module ID. The ID for the management module is 112.
Status	Displays the status of the module as one of the following:
VACANT	The slot is empty.
POWERED-OF	The module is present in the slot but is powered off.
POWERING UP	The module is present and powering on.
LOADING	The module is present, powered on, and loading the initial configuration.
INITIALIZING	The module is present, powered on, and initializing hardware components.
ENABLED	The module is on and fully enabled.
DISABLED	The module is powered on but disabled.
FAULTY	The module is faulty because an error was detected.
UNKNOWN	The module is inserted but its state cannot be determined.

Usage Guidelines Diagnostic tests (POST1, POST2) are not running on the management modules.

Examples To display the management modules present in a Brocade VDX 8770-4 chassis:

```
switch# show mm
Slot  Type         Description                ID      Status
------------------------------------------------------------------------
 M1   MM           Management Module          112     ENABLED
 M2                                                   VACANT
```

See Also show linecard, show sfm, show slots

show monitor

Displays the monitoring information for all Port Mirroring sessions.

Synopsis **show monitor**

show monitor session *session_number*

Operands **session** *session_number*

Specifies a session identification number. The range of valid values is from 0 to 23.

Defaults None

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 None

Examples To display monitoring information for all Port Mirroring sessions:

```
switch# show monitor
```

See Also monitor session

show name-server brief

Displays brief entries of local name server (NS) information about devices connected to a switch.

Synopsis **show name-server brief** [**rbridge-id** *rbridge-id*]

Operands

rbridge-id *rbridge-id*	Specifies the RBridge identifier of the switch for which the brief name server entries are displayed. If no RBridge identifier is specified brief entries for all devices in the fabric are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display local name server (NS) information about devices connected to a switch. Brief output lists only the Fibre Channel address (PID) of each device.

If no information is available for the switch, the command displays the message: “0 entries.”

Usage Guidelines None

Examples To view brief name server entries for all devices connected to a switch:

```
switch# show name-server brief
010000 020100 030200 010300 020400 030500 010600 020700 030800
```

To view brief name server entries for a specific switch:

```
switch# show name-server brief rbridge-id 3
030200 030500 030800
```

See Also show name-server detail, show name-server nodefind

show name-server detail

Displays local name server (NS) information about devices connected to a switch.

Synopsis **show name-server detail [rbridge-id** *rbridge-id*]

Operands

rbridge-id *rbridge-id* Specifies the RBridge identifier of the switch for which the details about name server entries are displayed. If no RBridge identifier is specified detail entries for all devices in the fabric are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays detailed local name server (NS) information about devices connected to a switch. The detail output contains the following information for each device:

PID Fibre Channel address of the device in 6-digit hexadecimal format.

Port Name Worldwide port name (WWPN) of the device.

Node Name Worldwide node name (WWNN) of the device.

SCR Indicates the State Change Registration of the device, which affects RSCN behavior. The value can be one of the following:

0 – No registration

1 – Fabric detected RSCN

2 – Port detected RSCN

3 – Both Fabric and Port detected RSCN

NOTE
This information is only available for devices that are connected to the local Rbridge on which the command is executed.

FC4s Fibre Channel FC4 type of the device represented as an ASCII string.

PortSymb User defined name for this port (ASCII string).

Fabric Port Name Fabric port name (worldwide name format). This is the F_Port worldwide name to which the N_Port connects.

Permanent Port Name

Physical Nx_Port worldwide name.

Device Type Type and role of the device, where the device type is either “Physical”, “Virtual”, “NPIV”, or “iSCSI”. The role is either “Initiator”, “Target”, or “Initiator + Target”. If the device role is not registered, the display indicates “unknown”. If the device registers a type that is not one of the aforementioned values, then the type is listed as “undefined”.

Interface Interface information for the port. For FCoE devices this information is shown as:

Fcoe *vlan/rbridge-id/FCoE port*

Physical Interface	Physical interface information for the port. For FCoE devices this information is shown as: Te *rbridge-id/slot/port* Where Te = Ten Gigabit Ethernet
Share Area	The state of the Brocade shared area addressing method. If “Yes” then the port uses shared area addressing.
Redirect	Indicates whether or not the device is involved in Brocade Frame Redirection. If “Yes” then the device is involved in Frame Redirection zoning.

If no information is available for the switch, the command displays the message: “total number of 0 entries.”

Usage Guidelines None

Examples To view name server entries for all devices connected to a switch:

```
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
```

See Also show name-server brief, show name-server nodefind

show name-server nodefind

Displays the local name server (NS) information for a specific device. The lookup is performed using either the Fibre Channel address (Port ID, or PID), or the worldwide name (WWN) of the device.

Synopsis **show name-server nodefind {PID** *pid* **| WWN** *wwn***}**

Operands

PID *pid*	Specifies the Fibre Channel address of the device to search for.
WWN *wwn*	Specifies the worldwide name of the device to search for.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display local name server (NS) information about a specific detailed entry.

See show name-server detail for descriptions of the displayed information.

If no information is available for the device, the command displays one of the following messages:

For PID lookup: `Device with PID of pid does not exist`

For WWN lookup: `Device with WWN of wwn does not exist`

Usage Guidelines None

Examples To view name server information for a device specified by PID:

```
switch# show name-server nodefind pid 0x012100
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
```

See Also show name-server brief, show name-server detail

show name-server zonemember

Displays the local name server (NS) zoning information.

Synopsis **show name-server zonemember** {**PID** *pid* | **WWN** *wwn*}

Operands

PID *pid*	Specifies the Fibre Channel address of the device.
WWN *wwn*	Specifies the worldwide name of the device.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display detailed local name server (NS) information about all devices zoned with the specified device. The lookup is performed using either the Fibre Channel address (Port ID, or PID), or the worldwide name (WWN) of the device.

Usage Guidelines If no information is available for the device, the command displays one of the following messages:

For PID lookup:	*Device with PID of pid does not exist*
For WWN lookup:	*Device with WWN of wwn does not exist*

Examples To view name server information for a device specified by PID:

```
switch# show name-server zonemember pid 0x010500
PID: 010500
Port Name: 10:00:00:05:1F:ED:95:38
Node Name: 20:00:00:05:1F: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: 20:21:00:05:1F:ED:79:7A
Permanent Port Name: 10:00:00:05:1F:ED:95:38
Device type: Physical Initiator
Interface: Fcoe 1/1/5
Physical Interface: Te 1/0/5
Share Area: No
Redirect: No

PID: 010600
Port Name: 10:00:00:05:1F:CD:95:38
Node Name: 20:00:00:05:1F:CD: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:CD:95:38
    Device type: Physical Initiator
    Interface: Fcoe 1/1/6
    Physical Interface: Te 1/0/6
    Share Area: No
    Redirect: No
```

See Also show name-server brief, show name-server detail, show name-server nodefind

show netconf client-capabilities

Displays the client capabilities associated with each NETCONF session.

Synopsis **show netconf client-capabilities**

Operands None

Defaults None

Command Modes Privileged-EXEC

Description This command displays client capabilities for all active NETCONF sessions. It always displays the session-ID, login name of the user of the client session, the host IP address, and the time the user logged on. The application vendor name, application product name and version number, and the identity of the client are also returned if these values are advertized by the client as capabilities in the <hello> message to the server at the start of the session.

Usage Guidelines None

Examples

```
switch# show netconf client-capabilities
Session Id : 10
User name  : root
Vendor     : Brocade
Product    : Brocade Network Advisor
Version    : 9.1.0 Build 123
Client user : admin-user
Host IP    : 10.24.65.8
Login time : 2011-08-18T08:54:24Z

Session Id : 11
User name  : root
Vendor     : Not Available
Product    : Not Available
Version    : Not Available
Client user   : Not Available
Host IP    : 10.24.65.8
```

See Also **show netconf-state capabilities, show netconf-state statistics**

show netconf-state capabilities

Displays NETCONF server capabilities.

Synopsis **show netconf-state capabilities**

Operands None

Defaults None

Command Modes Privileged-EXEC mode

Description This command displays the NETCONF capabilities supported by the NETCONF server.

Usage Guidelines None

Examples

```
switch# show netconf-state capabilities
netconf-state capabilities capability urn:ietf:params:netconf:base:1.0
netconf-state capabilities capability
urn:ietf:params:netconf:capability:writable-running:1.0
netconf-state capabilities capability
urn:ietf:params:netconf:capability:startup:1.0
netconf-state capabilities capability
urn:ietf:params:netconf:capability:xpath:1.0
netconf-state capabilities capability
urn:ietf:params:netconf:capability:validate:1.0
netconf-state capabilities capability
http://tail-f.com/ns/netconf/actions/1.0
netconf-state capabilities capability
http://tail-f.com/ns/aaa/1.1?revision=2010-06-17&module=tailf-aaa
netconf-state capabilities capability
urn:brocade.com:mgmt:brocade-aaa?revision=2010-10-21&module=brocade-aaa
(output truncated)
```

See Also **show netconf client-capabilities, show netconf-state datastores, show netconf-state schemas, show netconf-state sessions, show netconf-state statistics**

show netconf-state datastores

Displays the NETCONF datastores that are present on the NETCONF server.

Synopsis **show netconf-state datastores**

Operands None

Defaults None

Command Modes Privileged-EXEC mode

Description This command displays NETCONF datastores on the NETCONF server along with related locking information.

Usage Guidelines None

Examples

```
switch# show netconf-state datastores
         LOCKED                 LOCKED
         BY       LOCKED  LOCK  BY       LOCKED          LOCKED
NAME     SESSION  TIME    ID    SESSION  TIME    SELECT  NODE
-----------------------------------------------------------------
running  -        -
startup  -        -
```

See Also **show netconf-state capabilities, show netconf-state schemas, show netconf-state sessions, show netconf-state statistics**

show netconf-state schemas

Displays the data models supported by the NETCONF server.

Synopsis **show netconf-state schemas**

Operands None

Defaults None

Command Modes Privileged-EXEC mode

Description This command displays the data models supported by the NETCONF server.

Usage Guidelines None

Examples None

See Also **show netconf-state capabilities, show netconf-state datastores, show netconf-state sessions, show netconf-state statistics**

show netconf-state sessions

Displays information about currently active NETCONF sessions.

Synopsis **show netconf-state sessions**

Operands None

Defaults None

Command Modes Privileged-EXEC mode

Description This command displays the following information about each active NETCONF session:

- Transport used by the session
- Login name of the user
- Client IP address
- The lime the user logged in

This command also provides a summary of RPC error counts and notifications.

Usage Guidelines None

Examples

```
switch# show netconf-state sessions
etconf-state sessions session 6
transport cli-console
username admin
source-host 127.0.0.1
login-time 2011-09-05T11:29:31Z
netconf-state sessions session 9
transport netconf-ssh
username root
source-host 172.21.132.67
login-time 2011-09-05T11:50:33Z
in-rpcs 0
in-bad-rpcs 0
out-rpc-errors 0
out-notifications 0
```

See Also **show netconf-state capabilities, show netconf-state datastores, show netconf-state schemas, show netconf-state statistics**

show netconf-state statistics

Displays NETCONF server statistics.

Synopsis **show netconf-state statistics**

Operands None

Defaults None

Command Modes Privileged-EXEC mode

Description This command displays statistics related to the NETCONF server, including counts of the following entities

- Start time of the NETCONF server
- Erroneous <hello> elements received
- Client sessions begun
- Dropped sessions
- Remote procedure calls (RPCs) received
- Erroneous RPCs received
- RPC errors returned to clients
- Notifications sent

Usage Guidelines None

Examples

```
switch# show netconf-state statistics
netconf-state statistics netconf-start-time 2012-04-27T09:12:09Z
netconf-state statistics in-bad-hellos 0
netconf-state statistics in-sessions 3
netconf-state statistics dropped-sessions 0
netconf-state statistics in-rpcs 4
netconf-state statistics in-bad-rpcs 0
netconf-state statistics out-rpc-errors 0
netconf-state statistics out-notifications 0
```

See Also **show netconf-state capabilities, show netconf-state datastores, show netconf-state schemas, show netconf-state sessions**

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** [**rbridge-id** *rbridge-id* | **all**]

Operands **rbridge-id**

rbridge-id	Specifies the Rbridge ID on which the NTP server status displays.
all	For this release, specifying **all** returns only local information.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the active NTP server. If an NTP server is not configured, the command output displays the server as “LOCL”. Otherwise, the command displays the NTP server IP address.

Usage Guidelines The request is for the local switch only.

Examples To show the local switch NTP status when an NTP server is not configured:

```
switch# show ntp status
rbridge-id 1: active ntp server is LOCL
```

To show the configured NTP server:

```
switch# show ntp status
active ntp server is 10.31.2.81
```

See Also **ntp server**

show policymap

Displays configured policy-maps and class-map Policer parameters applied to switch interfaces.

Synopsis **show policymap interface tengigabitethernet** *rbridge-id/slot/port* **input | output**

Operands **interface tengigabitethernet** *rbridge-id/slot/port* (Interface where policy-map is bound.)

input | output Direction (inbound or outbound) where policy applied.

Defaults None

Command Modes global configuration mode

interface configuration mode

Description Use this command to display configured policy-maps bound to switch interfaces.

Usage Guidelines Using **show policymap** for a specific interface. This displays policy-map binding settings (policy-map name and traffic direction), police-priority-map applied, and class-map Policer parameters applied for that interface. Using **show policymap** without identifying an interface and direction of traffic displays policy-map binding for all interfaces on the switch.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To display policy-map binding and class-map parameters applied to a specific interface:

```
switch# show policymap interface tengigabitethernet 4/1 in
Interface : TenGigabitEthernet 4/1
Policymap: policymapA-1
Direction: Input
Input Excluded lossless priorities: None

Class-map: default
  Police:
    cir 5 bps cbs 5678 bytes eir 512000 bps ebs 4096 bytes
    Police-priority-map: po-pr-map1
    Conformed: 30720 bytes set-dscp 0 set-tc 0
    Exceeded: 23424 bytes set-dscp 0 set-tc 0
    Violated: 0 bytes
    Total: 54144 bytes
```

To display policy-map binding information for all switch interfaces:

```
switch# show policymap
Interface : TenGigabitethernet 4/2
Inbound policy map is policymapA-1
Outbound policy map is not set

Interface : TenGigabitethernet 4/3
Inbound policy map is not set
Outbound policy map is not set

Interface : TenGigabitethernet 4/4
Inbound policy map is not set
Outbound policy map is not set
```

Example definitions

Following are definitions of terms used in output from the **show policymap** command:

- Interface–The interface for which rate limiting information is being displayed.
- Direction–The traffic direction for which rate limiting is applied.
- police-priority-map–remarked priority-map used for Policer application (802.1 p priority remarked map).
- Conform–The traffic in bytes that has been forwarded from this interface that is within the CIR bandwidth limits.
- Exceeded–The traffic that has been exceeded the bandwidth available in the CIR limits and has not exceed the EIR limits for this rate-limit policy.
- Violated–The traffic that has exceeded the bandwidth available in the CIR and EIR limits.
- set-dscp–The DSCP value which is applied to the traffic for the given color (conform, exceed, violate).
- set-tc–The remapped traffic class queue for the traffic for the given color (conform, exceed, violate).
- Total –The total traffic in bytes carried on this interface for the defined rate-limit policy.

See Also show running-config policy-map, policy-map, class, qos cos, show running-config class-map

show port port-channel

Displays the detailed LACP attributes.

Synopsis **show port port-channel** *port_id*

Operands *port_id* Port to display.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the detailed LACP attributes that are configured and negotiated with its partner.

Usage Guidelines None

Examples None

See Also None

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 for standalone mode. The range of valid values is from 1 through 6144 for Brocade VCS Fabric mode.

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.

***** The asterisk designates that the designated port channel is the egress for BUM traffic.

Defaults None

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 38
 LACP Aggregator: Po 38
 Aggregator type: Standard
  Admin Key: 0038 - Oper Key 0038
  Partner System ID - 0x8000,01-e0-52-00-20-00
  Partner Oper Key 0038
 Member ports:
   Link: Te 0/13 (0x180D0102) sync: 1
   Link: Te 0/14 (0x180E0103) sync: 1   *
```

See Also None

show port-profile

Displays the AMPP port-profile configuration information.

Synopsis **show port-profile**

Operands None

Description Use this command to display the port profile configuration information.

Defaults None

Command Modes Privileged EXEC mode

Usage Guidelines None

Examples

```
switch# show port-profile
port-profile default
ppid 0
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
port-profile auto-dvPortGroup-2
ppid 1
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan add 45
port-profile auto-dvPortGroup-1
ppid 2
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3-10
```

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** | **port-channel** *channel-group-number* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands

all	Displays the port-profile information for all interfaces.
port-channel *channel-group-number*	Specifies a LAG port channel-group number to display. The range of valid values is from 1 through 63 for standalone mode. The range of valid values is from 1 through 6144 for Brocade VCS Fabric mode.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

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 None

Examples None

See Also show running-config, show port-profile, show port-profile status

show port-profile name

Displays the port profile information for a named port-profile.

Synopsis **show port-profile name** *port-profile-name* {**qos** | **security** | **status** | **vlan**}

show port-profile name *port-profile-name* **name** *port-profile-name* **validate**

Operands

port-profile-name		The name of the port profile. The maximum number of characters is 64.
	qos	QoS sub-profile
	security	Security sub-profile
	status	Specific port-profile status
	vlan	Vlan sub-Profile
validate		Validates two port-profiles against each other.

Defaults None

Command Modes Privileged EXEC mode

Description Displays the port profile information for a named port-profile.

Usage Guidelines None

Examples None

See Also 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.
associated	Show all port-profiles with the **associated** status for the given profile.
applied	Show all port-profiles with the **applied** status for the given profile.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the port-profile status.

Usage Guidelines Use the **show port-profile** version of this command to display the status of all AMPP profiles.

Examples

```
switch# show port-profile status
Port-Profile           PPID     Activated     Associated MAC      Interface
auto-dvPortGroup-2     1        Yes           0050.5681.2ed5      none
                                              0050.5699.5524      te0/2
                                              0050.5699.39e0      te0/1
auto-dvPortGroup-1     2        Yes           0050.5681.083c      none
```

See Also show running-config, show port-profile, show port-profile interface

show process cpu

Displays information about the active processes in the switch and their corresponding CPU utilization statistics.

Synopsis **show process cpu** [**rbridge-id** {*rbridge-id* | **all**}] [**summary**]

Operands

cpu		Displays processes by percent of CPU usage.
	summary	Displays a summary view of cpu usage.
rbridge-id		Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
	rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID
	all	Specifies all switches in the fabric. This option is not supported.

Defaults None

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 This command is supported only on the local switch.

For an explanation of process states, refer to the UNIX manual page for the **ps** command.

Examples To show the information for all processes:

```
switch# show process cpu summary
Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.03; Fifteen minutes: 0.01
```

To show CPU usage information by individual processes:

```
switch# show process cpu
Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.02; Fifteen minutes: 0.00

Active Processes Lifetime Statistic:
  PID   Process          CPU%  State      Started
17169   sh                1.00    S       13:44:27 Jul  1, 2012
 2060   emd               0.80    S       21:52:27 Jun 29, 2012
 2462   SWITCH_TMR_0      0.60    S       21:53:08 Jun 29, 2012
17170   imishow_proc_cp   0.50    S       13:44:27 Jul  1, 2012
 2207   ospfd             0.20    S       21:52:41 Jun 29, 2012
 2211   mstpd             0.20    S       21:52:41 Jun 29, 2012
 2208   rtmd              0.10    S       21:52:41 Jun 29, 2012
(output truncated)
```

See Also **show process memory**, show process info

show process info

Displays system processes hierarchically.

Synopsis **show process info** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

info	**Displays system processes hierarchically.**
rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display system processes in hierarchical order.

Usage Guidelines Pagination is not supported with this command. Use the more option to display the output one page at a time.

This command is supported only on the local switch.

Examples To display system processes hierarchically:

```
switch# show process info
PID     CMD
2       kthreadd
3       \_ migration/0
4       \_ ksoftirqd/0
5       \_ watchdog/0
6       \_ migration/1
7       \_ ksoftirqd/1
8       \_ watchdog/1
9       \_ migration/2
10      \_ ksoftirqd/2
11      \_ watchdog/2
12      \_ migration/3
13      \_ ksoftirqd/3
14      \_ watchdog/3
15      \_ migration/4
16      \_ ksoftirqd/4
17      \_ watchdog/4
18      \_ migration/5
19      \_ ksoftirqd/5
20      \_ watchdog/5
21      \_ migration/6
22      \_ ksoftirqd/6
(output truncated)
```

See Also **show process cpu, show process memory**

show process memory

Displays the memory usage information based on processes running in the system.

Synopsis **show process memory** [**rbridge-id** {*rbridge-id* | **all**}] [**summary**]

Operands

memory	**Displays processes by memory usage (in KB).**
summary	Displays a summary view of memory usage.
rbridge-id	Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode. This option is supported only for the local RBridge ID.
all	Specifies all switches in the fabric. This option is not supported.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view memory usage information based on processes running in the system.

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

Examples To show a summary of memory usage by all processes:

```
switch# show process 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 process memory
%Memory Used: 16.0338%; TotalMemory: 6191792 KB; Total Used: 992780 KB; Total
Free: 5198764 KB
  PID   Process          MEM%   Mem Used(bytes)
    1   init             0.00           1937408
    2   kthreadd         0.00                 0
    3   migration/0      0.00                 0
    4   ksoftirqd/0      0.00                 0
    5   watchdog/0       0.00                 0
    6   migration/1      0.00                 0
    7   ksoftirqd/1      0.00                 0
    8   watchdog/1       0.00                 0
    9   migration/2      0.00                 0
   10   ksoftirqd/2      0.00                 0
   11   watchdog/2       0.00                 0
   12   migration/3      0.00                 0
   13   ksoftirqd/3      0.00                 0
   14   watchdog/3       0.00                 0
   15   migration/4      0.00                 0
   16   ksoftirqd/4      0.00                 0
   17   watchdog/4       0.00                 0
   18   migration/5      0.00                 0
```

See Also **show process cpu**, show process info

show prom-access

Shows the Boot PROM access status.

Synopsis **show prom-access**

Operands None

Defaults By default, the boot PROM is accessible.

Command Modes Privileged EXEC mode

Description Use this command to determine whether the Boot PROM is accessible.

Under non-FIPS compliant operation, you can access the Boot PROM by holding down the ESC key during the 4-second period when the switch is booting up. In FIPS compliant state, PROM access is disabled to prevent users from net-installing firmware.

If PROM access is enabled, you can disable it in preparation for FIPS compliance. If PROM access is disabled, you cannot re-enable it.

Enter the **unhide fips** command with password "**fibranne**" to make the command available.

Usage Guidelines None

Examples To view the Boot PROM access status:

```
switch# show prom-access
PROM access Enabled
```

See Also prom-access disable, cipherset, fips root disable, fips selftests, fips zeroize, unhide fips

show qos flowcontrol interface

Displays all of the configured flow control information for an interface.

Synopsis **show qos flowcontrol interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **all**]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
all	Reports QoS flow control statistics for all interfaces within the system.

Defaults None

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.

The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display all of the configured flow control information for a 10 Gbps Ethernet interface:

```
switch#show qos flowcontrol interface tengigabitethernet 5/0/1
Interface TenGigabitEthernet 5/0/1
  Mode PFC
  DCBX enabled for PFC negotiation
  TX 0 frames
         TX   TX    RX   RX Output Paused
  CoS Admin Oper 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
```

See Also show qos interface, show cee maps

show qos interface

Displays a summary of all QoS configurations applied on an interface.

Synopsis **show qos interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **all**]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge ID.
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 None

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.

The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display all of the configured QoS information for a 10 Gbps Ethernet interface:

```
switch# show qos interface tengigabitethernet 22/0/1
Interface TenGigabitEthernet 22/0/1
  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      3      4      5      6      7
     ------------------------------------------------------------------
```

```
     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    7
     ------------------------------------------------
Threshold:      64   64   64   64   64   64   64   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   0
  Multicast Packet Expansion Traffic Class Scheduler
TrafficClass:    0    1    2    3    4    5    6    7
     ------------------------------------------------
DWRRWeight:     25   25   25   25   25   25   25   25
```

See Also cee-map (FCoE)

show qos maps

Displays information on the defined QoS maps.

Synopsis **show qos 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 None

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 maps dscp-cos

Displays configured DSCP-CoS maps.

Synopsis **show qos maps dscp-cos**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured qos DSCP-CoS maps.

Usage Guidelines None

Examples To display information on defined qos DSCP-CoS maps and application on interfaces.

```
sw0# show qos maps dscp-cos
Dscp-to-CoS map 'test' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------
 0 :    00 03 07 03 07 03 07 03 07 01
 1 :    01 05 06 05 06 05 06 05 06 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 04 04 04 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07
Enabled on the following interfaces:
    Te 16/2/2
```

This information relates to the following map configuration applied to interface 16/2/2:

```
qos map dscp-mutation test
mark 1,3,5,7 to 3
mark 11,13,15,17 to 5
mark 12,14,16,18 to 6
mark 2,4,6,8 to 7
```

See Also qos map dscp-cos

show qos maps dscp-mutation

Displays configured DSCP-mutation maps.

Synopsis **show qos maps dscp-mutation**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured qos DSCP-mutation maps and application on interfaces.

Usage Guidelines This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To display information on defined QoS DSCP-mutation maps.

```
sw0# show qos maps dscp-mutation
Dscp-to-Dscp Mutation map 'test' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------
 0 :    00 09 10 09 10 09 10 09 10 09
 1 :    10 19 20 19 20 19 20 19 20 19
 2 :    20 21 22 23 24 25 26 27 28 29
 3 :    30 31 32 33 34 35 36 37 38 39
 4 :    40 41 42 43 44 45 46 47 48 49
 5 :    50 51 52 53 54 55 56 57 58 59
 6 :    60 61 62 63
Enabled on the following interfaces:
    Te 16/2/2
```

This information relates to the following map configuration applied to interface 16/2/2:

```
qos map dscp-mutation test
mark 1,3,5,7 to 9
mark 11,13,15,17 to 19
mark 12,14,16,18 to 20
mark 2,4,6,8 to 10
```

See Also qos map dscp-mutation

show qos maps dscp-traffic-class

Displays configured DSCP-Traffic-Class maps.

Synopsis **show qos maps dscp-traffic-class**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured QoS DSCP-Traffic-Class map and application on interfaces.

Usage Guidelines None

Examples To display information on defined qos dscp-mutation maps.

```
sw0# show qos maps dscp-traffic-class
Dscp-to-Dscp Mutation map 'test' (dscp= d1d2)
Dscp-to-Traffic Class map 'pqrs'(dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------
 0 :    00 03 07 03 07 03 07 03 07 01
 1 :    01 05 06 05 06 05 06 05 06 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 04 04 04 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07
Enabled on the following interfaces:
    Te 16/2/2
```

This information relates to the following map configuration applied to interface 16/2/2:

```
qos map dscp-mutation test
mark 1,3,5,7 to 3
mark 11,13,15,17 to 5
mark 12,14,16,18 to 6
mark 2,4,6,8 to 7
```

See Also 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 qos queue interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **all**]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
all	Reports QoS statistics for all Ethernet interfaces within the system.

Defaults None

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).

The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display the queueing information for a **10 Gbps Ethernet interface**:

```
switch# show qos queue interface tengigabitethernet 5/0/2
Interface TenGigabitEthernet 5/0/2
                RX              RX                    TX              TX
  CoS       Packets           Bytes      TC       Packets           Bytes
  ------------------------------      ------------------------------
    0        680458        87098624       0             0               0
    1             0               0       1         32318               0
    2             0               0       2             0               0
    3             0               0       3             0               0
    4             0               0       4             0               0
    5             0               0       5             0               0
    6             0               0       6             0               0
    7             0               0       7             0               0
```

See Also qos map cos-mutation, cee-map (configuration)

show qos rcv-queue interface

Displays a summary the runtime ingress queue state information.

Synopsis **show qos rcv-queue interface** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **all**]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
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 None

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 The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

This command, however, is not supported on VDX 8770-4 and VDX 8770-8 platforms.

Examples To display the runtime ingress queue state information retrieved from the dataplane for a 10 Gbps Ethernet interface:

```
switch# show qos rcv-queue interface tengigabitethernet 22/0/2
Interface TenGigabitEthernet 22/0/2
  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 qos rcv-queue multicast

show qos 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 qos rcv-queue multicast** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **all**]

Operands

tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
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 None

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 This command is not supported on VDX 8770-4 and VDX 8770-8 platforms.

For a stand-alone switch, all ASICs are considered as slot number zero (0).

The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display the queueing information:

```
switch# show qos rcv-queue multicast tengigabitethernet 1/0/2
Dropped Counts
  Linecard/Portset          TC 0          TC 1          TC 2          TC
3
--------------------------------------------------------------------------------

0/0                   0             0             0             0
```

See Also show qos rcv-queue interface

show qos red profiles

Displays configured random early discard (RED) profiles.

Synopsis **show qos red profiles**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured RED profiles and application on interfaces.

Usage Guidelines This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To display information on defined qos RED profiles use **show qos red profiles**. Note that the first example shows output for the RED profile configured in the example under "qos red profile" on page 343.

```
switch# show qos red profiles

Red Profile 2
        Minimum Threshold: 10
        Maximum Threshold: 80
        Drop Probability: 80

Activated on the following interfaces:
Te 1/2/2  CoS: 7

Red Profile 100
        Minimum Threshold: 30
        Maximum Threshold: 80
        Drop Probability: 56

Activated on the following interfaces:
Te 1/1  CoS: 2

Red Profile 200
        Minimum Threshold: 40
        Maximum Threshold: 60
        Drop Probability: 40

Activated on the following interfaces:
Te 1/1  CoS: 4
```

To examine the applied RED profiles for a specific interface, use the **show qos interface** *interface-name* command:

```
switch# show qos interface te 1/2/2
Interface TenGigabitEthernet 1/2/2
  Provisioning mode non-cee
  Default CoS 0
  Interface COS trust untrusted
  CoS-to-CoS Mutation map 'default'
  CoS-to-Traffic Class map 'default'
                  In-CoS:   0   1   2   3   4   5   6   7
```

```
    ------------------------------------------------
    Out-CoS/TrafficClass: 0/1 0/1 0/1 0/1 0/1 0/1 0/1 0/7
  Interface DSCP trust untrusted
  DSCP-to-DSCP Mutation map 'default' (dscp= d1d2)
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
  -----------------------------------
   0 :    00 01 02 03 04 05 06 07 08 09
   1 :    10 11 12 13 14 15 16 17 18 19
   2 :    20 21 22 23 24 25 26 27 28 29
   3 :    30 31 32 33 34 35 36 37 38 39
   4 :    40 41 42 43 44 45 46 47 48 49
   5 :    50 51 52 53 54 55 56 57 58 59
   6 :    60 61 62 63

  RED Enabled on the following Priorities:
        CoS: 7, Profile: 2
more
```

See Also qos red profile

show qos red statistics interface

Displays RED statistics for a specific interface.

Synopsis **show qos red statistics interface** *interface-name*

Operands *interface-name* Name of interface where RED profile applied.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display statistics for RED on a specific interface where a RED profile is applied. Statistics include packets and bytes dropped for the CoS priority mapped to the profile for the interface.

Usage Guidelines None

Examples To display RED statistics on interfaces use the **show qos red statistics interface** *interface-name* command. Note that the colors in the following example (red, yellow, and green) relate to color based priority mapping set through the Port-Based Policer feature. Refer to the *Network OS Administrator's Guide* for more information.

```
switch# show qos red statistics interface Te 2/1
Statistics for interface: Te 2/1
CoS: 2, ProfileId: 20
    Packets Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
    Bytes Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
CoS: 3, ProfileId: 10
    Packets Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
    Bytes Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
```

See Also qos red profile, show qos red profiles

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 None

Command Modes Privileged EXEC mode

Description Use this command to display the status of the current RMON on the switch.

Usage Guidelines None

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:

```
switch# show rmon events
event Index = 4
        Description "My Description"
        Event type Log & SnmpTrap
        Event community name admin
        Last Time Sent = 00:00:00
        Owner  admin
```

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 None

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 reserved-vlan

Displays the range of reserved VLAN values.

Synopsis **show running reserved-vlan**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the range of reserved VLAN values.

Usage Guidelines None

Examples None

See Also **reserved-vlan, show default-vlan**

show running-config

Displays the contents of the running configuration.

Synopsis **show running-config**

Operands Refer to the usage guidelines.

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.

Use the **show running-config?** command to display the list of available configuration entries.

Use the **show vcs virtual-ip** command to display the virtual IP address.

Examples To display the running configuration:

```
switch# show running-config
chassis virtual-ip 10.24.73.50/20
no diag post enable
linecard 2 LC48x10G
linecard 4 LC48x10G
class-map default
 match any
!
logging rbridge-id 1
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
switch-attributes 1
 chassis-name VDX8770-4
 host-name sw0
!
support rbridge-id 1
 ffdc
!
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common!
[output truncated]
```

See Also show startup-config, show startup-db

show running-config aaa

Display the AAA server configuration.

Synopsis **show running-config aaa**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to displays the configuration attributes for authentication, authorization, and accounting (AAA) from the configuration database.

Usage Guidelines Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples To displaying the authentication mode:

```
switch# show running-config aaa
aaa authentication radius local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none
```

See Also **aaa authentication**

show running-config aaa accounting

Display the AAA server accounting configuration.

Synopsis **show running-config aaa accounting**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to displays the configuration attributes AAA accounting services.

Usage Guidelines Refer to the **aaa accounting** command for a description of the displayed attributes.

Examples To displaying the authentication mode:

```
switch# show running-config aaa accounting
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

See Also **aaa authentication, aaa accounting**

show running-config access-list ip

Displays IP ACLs in the running configuration.

Synopsis **show running-config access-list ip** [**acl-name** *name*]

Operands **acl-name** *name* Specifies a MAC ACL.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the rules of IP ACLs in the running configuration.

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

Examples To display all IP ACLs in the running-config of the local switch:

```
switch# show running-config access-list ip
Interface TenGigabitEthernet 2/1
   Inbound access-list is IP_ACL_STD_EXAMPLE (From User)
   Outbound access-list is IP_ACL_EXT_EXAMPLE (From User)
```

See Also mac access-list extended, mac access-list standard

show running-config access-list mac

Displays MAC ACLs in the running configuration.

Synopsis **show running-config access-list mac** [**acl-name** *name*]

Operands **acl-name** *name* Specifies a MAC ACL.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the rules of MAC ACLs in the running configuration.

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

Examples To display all MAC ACLs in the running-config of the local switch:

```
switch# show running-config access-list mac
mac access-list extended haha
 seq 10 deny 0000.0000.0011 0000.0000.0022
mac access-list extended ww
 seq 10 deny 0000.0000.1101 any 8100
rw
```

See Also mac access-list extended, mac access-list standard

show running-config banner

Displays the switch banner.

Synopsis **show running-config banner**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the banner test string configured for the switch.

Usage Guidelines None

Examples To display the switch banner:

```
switch# show running-config banner
banner login “Please don’t disturb the setup on this switch.”
```

See Also **banner login**

show running-config cee-map

Displays the Converged Enhanced Ethernet (CEE) map.

Synopsis **show running-configuration cee-map** [**precedence** | **priority-group-table** [*pgid*]| **priority-table** | **remap** {**fabric-priority** | **lossless-priority**}]

Operands

precedence	Displays only the precedence of the default CEE map.
priority-group-table	Without a specified priority group ID, displays the priority group table for each priority group ID.
pgid	Specifies one priority group ID.
priority-table	Displays the configured priority table map.
remap fabric-priority	Displays the fabric priority for the Brocade VCS Fabric QoS.
remap lossless-priority	Displays the lossless priority for the Brocade VCS Fabric QoS.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display properties of the configured CEE map. Without parameters, the command displays the precedence of the default CEE map, priority group table for each priority group ID, the configured priority table map, and the fabric priority and lossless priority for the Brocade VCS Fabric QoS.

Usage Guidelines None

Examples To display the CEE map:

```
switch(config)# show running-configuration cee-map
cee-map default
precedence 1
 priority-group-table 1 weight 40 pfc on
 priority-group-table 15.0 pfc off
 priority-group-table 15.1 pfc off
 priority-group-table 15.2 pfc off
 priority-group-table 15.3 pfc off
 priority-group-table 15.4 pfc off
 priority-group-table 15.5 pfc off
 priority-group-table 15.6 pfc off
 priority-group-table 15.7 pfc off
 priority-group-table 2 weight 60 pfc off
 priority-table 2 2 2 1 2 2 2 15.0
 remap fabric-priority priority 0
 remap lossless-prioirty priority 0
!
```

See Also priority-group-table, remap fabric-priority, remap lossless-priority

show running-config class-map

Displays configured priority-maps.

Synopsis **show running-config class-map**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured police class-maps.

Usage Guidelines This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To display i defined QoS DSCP-mutation maps.

```
switch# show running-config class-map
class-map default
     match any
```

See Also qos cos

show running-config diag post

Displays the defined POST configuration.

Synopsis **show running-config diag post**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the POST configuration.

Usage Guidelines None

Examples

```
switch# show running-config diag post
diag post rbridge-id 132
     no enable
!

switch# show running-config diag post
diag post rbridge-id 132
     enable
!
switch#
```

See Also **diag post enable**

show running-config dot1x

Displays the IEEE 802.1x Port Authentication configuration.

Synopsis **show running-configuration dot1x** [**enable** | **test timeout**]

Operands

enable	Shows the configured state of globally enabled IEEE 8.02.1x port authentication.
test timeout	Shows the configured timeout value in seconds for the 802.1x readiness check.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display IEEE 802.1x Port Authentication information.

Usage Guidelines None

Examples None

See Also **dot1x enable, dot1x test timeout**

show running-config dpod

Displays license information.

Synopsis **show running-config dpod** [*rbridge-id/slot/port*]

Operands

rbridge-id	*Specifies a switch by its RBridge identifier.*
slot	Specifies the slot number.
port	Specifies the port number.

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 has no effect on the Brocade VDX 6710 and VDX 8770 platforms. These platforms do not support the Dynamic POD feature.

In the Network OS v3.0.0 release this command is supported only on the local RBridge.

Examples To display port reservations for all ports on the local switch:

```
switch# show running-config dpod
dpod 10/0/1
  reserve
!
dpod 10/0/2
  reserve
!
dpod 10/0/3
!
dpod 10/0/4
  reserve
!
dpod 10/0/5
!
dpod 10/0/6
  reserve
!
(output truncated)
```

To display port reservations on a switch that does not support the DPOD feature:

```
switch# show running-config dpod
%No entries found
```

See Also dpod, show dpod

show running-config fabric route mcast

Displays fabric route multicast configuration information.

Synopsis **show running-config fabric route mcast** {**rbridge-id** *rbridge-id* | **priority**}

Operands

rbridge-id *rbridge-id*	Specifies a switch by its RBridge identifier.
priority *value*	Displays the priority value.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display fabric route multicast configuration information.

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 rbridge-id 2

switch# show running-config fabric route mcast rbridge-id 2 priority
fabric route mcast rbridge-id 2
 priority 1
```

See Also **fabric route mcast**, 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 None

Command Modes Privileged EXEC mode

Description This command displays the currently running configuration for FCoE.

Usage Guidelines None

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 fcsp auth

Displays the protocol specific values.

Synopsis **show running-config fcsp auth**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the E_Port-to-EX_Port authentication protocol parameters such as auth-type, group, hash type and policy state.

Usage Guidelines The policy status can be one of the following. ON, OFF, ACTIVE, or PASSIVE. Refer to the **fcsp auth** command for a description of policy states.

Examples

```
switch# show running-config fcsp auth
fcsp auth group 2
fcsp auth hash md5
fcsp auth policy switch off
```

See Also **fcsp auth, fcsp auth-secret, show fcsp auth-secret dh-chap**

show running-config interface fcoe

Displays the status of FCoE interfaces.

Synopsis **show running-configuration interface fcoe** [*rbridge-id* | *slot* | *port*]

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of FCoE interfaces.

Usage Guidelines None

Examples

```
switch# show running-config interface fcoe
interface Fcoe 1/22/1
 no shutdown
!
interface Fcoe 1/22/2
 no shutdown
!
interface Fcoe 1/22/3
 no shutdown
!
interface Fcoe 1/22/4
 no shutdown
!
interface Fcoe 1/22/5
 no shutdown
!
interface Fcoe 1/22/6
 no shutdown
!
```

See Also None

show running-config interface FibreChannel

Displays Fibre Channel port attributes.

Synopsis **show running-config interface FibreChannel** [*rbridge-id/slot/port* **[desire-distance | fill-word | isl-r_rdy | long-distance | shutdown | speed | trunk-enable | vc-link-init]]**

Operands

rbridge-id	*Specifies a switch by its RBridge identifier.*
slot	Specifies a valid slot number.
port	Specifies a valid port number.
desire-distance	Displays the setting of the desired distance attribute.
fill-word	Displays the configured link initialization and fill word primitives for 8-GB Fibre Channel ports: idle-idle, arbff-arbff, idle-arbff, or aa-then-ia.
isl-r_rdy	Displays whether R_RDY buffer-to-buffer flow control is enabled for the ISL. VC_RDY flow control is enabled if R_RDY flow control is disabled.
long-distance	Displays the configured long distance mode: **l0**—Long distance mode is not configured. **le**—Link is up to 10 km. **ld**—Distance is determined dynamically. **ls**—Distance is determined statically by the user (**desire-distance** command).
shutdown	Displays whether the port is enabled (**no shutdown**) or disabled (**shutdown**).
speed	Displays the configured port speed: auto, 1 Gbps, 2 Gbps, 4 Gbps, or 8 Gbps.
trunk-enable	Displays whether trunking is enabled on the port.
vc-link-init	Displays the configured long distance fill word: **idle** or **arb**.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display port attributes for a specified Fibre Channel port or for all Fibre Channel ports on the cluster.

Enter the command without specifying *rbridge-id/slot/port* to obtain a listing of attributes for all Fibre Channel ports. Enter the command with the *rbridge-id/slot/port* parameters to obtain attributes information for a specific port. The values for desire-distance, isl-r_rdy, trunk-enable, and shutdown are always displayed. The values for fill-word, long-distance, speed, and vc-link-init are displayed only if they have been changed from their default values.

Include the attribute name to obtain the setting of that specific attribute only.

Use the **interface FibreChannel** command to set the values.

Usage Guidelines This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples To display Fibre Channel port attributes for all ports on a Brocade VDX 6730 switch:

```
switch# show running-config interface FibreChannel
interface FibreChannel 3/0/1
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 no shutdown
!
interface FibreChannel 3/0/2
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 no shutdown
!
interface FibreChannel 3/0/3
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 no shutdown
!
(output truncated)
```

To display Fibre Channel port attributes for one port of a Brocade VDX 6730 switch:

```
switch# show running-config interface FibreChannel 8/0/1
interface FibreChannel 8/0/1
 speed 8gbps
 long-distance ld
 vc-link-init arb
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 shutdown
!
```

To display the setting of a specific attribute on a specific port:

```
switch# show running-config interface FibreChannel 66/0/1 speed
interface FibreChannel 66/0/1
 speed auto
!
```

See Also desire-distance, fill-word, interface, isl-r_rdy, long-distance, shutdown, speed (Fibre Channel), trunk-enable, vc-link-init

show running-config interface gigabitethernet

Displays the status of 1 GB Ethernet interfaces.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id* | *slot* | *port*]

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults By default this command displays the configuration of all 1 GB interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of 1 GB Ethernet interfaces.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display configuration information about all 1GB Ethernet interfaces on the local switch:

```
switch# show running-config interface gigabitethernet
interface GigabitEthernet 22/0/1
 description tests
 channel-group 2 mode active type standard
 lacp timeout long
 sflow enable
 no shutdown
!
interface GigabitEthernet 22/0/2
 channel-group 2 mode active type standard
 lacp timeout long
 no shutdown
!
interface GigabitEthernet 22/0/3
 channel-group 2 mode active type standard
 lacp timeout long
 no shutdown
!
interface GigabitEthernet 22/0/4
 no shutdown
!
interface GigabitEthernet 22/0/5
 no shutdown
!
interface GigabitEthernet 22/0/6
 no shutdown
!
interface GigabitEthernet 22/0/7
 no shutdown
(output truncated)
```

See Also interface

show running-config interface gigabitethernet bpdu-drop

Displays the BPDU drop status of a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id* | *slot* | *port*] **bpdu-drop [enable]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
enable	Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display information about dropped BPDUs on the specified Ethernet interface.

Usage Guidelines STP, RSTP, or MSTP must be configured.

This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Brocade Network OS v3.0.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples To display BPDU drop status information for a specific 1 GB Ethernet port:

```
switch# show running-config interface gigabitethernet 1/0/7 bpdu-drop
```

See Also **interface**

show running-config interface gigabitethernet channel-group

Displays channel group configuration information for an interface participating in link aggregation.

Synopsis **show running-config interface gigabitethernet [** *rbridge-id* | *slot* | *port* **] channel-group [mode | type]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
mode	Displays the mode of link aggregation (active, passive, or on).
type	Displays the type of link aggregation (802.3ad standard-based LAG, or Brocade proprietary hardware-based trunking).

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display information about the channel group configuration of the specified Ethernet interface.

Usage Guidelines This command is relevant only to interfaces configured as part of a LAG.

This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples None

See Also **channel-group**

show running-config interface gigabitethernet description

Displays the description string associated with a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **description**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display the description string associated with the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/7 description
interface GigabitEthernet 1/0/7
 description Connects to storage device 1
!
```

See Also **description (interfaces), interface**

show running-config interface gigabitethernet dot1x

Displays IEEE 802.1x port-based access control configuration information for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id | slot | port* **dot1x [authentication | port-control | protocol-version | quiet-period | reauthMax | reauthentication | timeout [re-authperiod | server-timeout | supp-timeout | tx-period]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
authentication	Indicates whether 802.1x port-based access control is enabled on the interface.
port-control	Displays the status of port authorization: auto (authentication on the port is enabled), forced authorize, or force unauthorize.
protocol-version	Displays the version number of the dot1x protocol.
quiet-period	Displays the number of seconds between a failed authentication and the next authentication retry.
reauthMax	Displays the maximum number of reauthentication attempts before the port goes into the reauthorized state.
reauthentication	Indicates whether reauthentication is enabled on a port.
timeout	Displays 802.1x timeout values.
re-authperiod	Displays the reauthentication interval in seconds.
server-timeout	Displays the number of seconds the switch waits for a response from the authentication server.
supp-timeout	Displays the number of seconds that the switch waits for a response to the Extensible Authentication Protocol (EAP) frame.
tx-period	Displays the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before retransmitting the request

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display configuration information for an interface configured for IEEE 802.1x port-based access control.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display the 802.1x port-based authentication configuration for a 1 GB Ethernet interface:

```
switch# show running-config interface gigabitethernet 1/0/7 dot1x
interface GigabitEthernet 1/0/7
 dot1x authentication
 dot1x port-control auto
 dot1x quiet-period 120
 dot1x reauthMax 5
 dot1x reauthentication
 dot1x timeout server-timeout 60
!
```

See Also dot1x authentication, dot1x port-control, dot1x quiet-period, dot1x reauthentication, dot1x reauthMax, dot1x timeout re-authperiod, dot1x timeout server-timeout, dot1x timeout supp-timeout, dot1x timeout tx-period

show running-config interface gigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **lacp [timeout]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
timeout	Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display LACP settings for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples None

See Also **lacp timeout**

show running-config interface gigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **lldp [dcbx-version | disable | iscsi-priority | profile]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
dcbx-version	Displays the configured version of the Data Center Bridging Exchange (DCBX) protocol.
disable	Indicates whether LLDP is disabled on the interface.
iscsi-priority	Displays the configured priority that will be advertized in the DCBX iSCSI TLV.
profile	Displays the LLDP profile configured on the interface.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display Link Layer Discovery Protocol (LLDP) configuration information for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples None

See Also **lldp dcbx-version, lldp disable, lldp iscsi-priority, lldp profile**

show running-config interface gigabitethernet mac

Displays configured MAC parameters for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **mac [access-group]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
access-group	Displays MAC ACLs configured for the specified interface.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display configured MAC parameters for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples None

See Also **mac access-group**

show running-config interface gigabitethernet mtu

Displays the configured MTU for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **mtu**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display the configured MTU for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 mtu
interface GigabitEthernet 1/0/8
 mtu 2500
!
```

See Also **ip mtu**

show running-config interface gigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **port-profile-port**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display whether AMPP port-profiling is configured for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 port-profile-port
interface GigabitEthernet 1/0/8
 port-profile-port
!
```

See Also **port-profile-port**

show running-config interface gigabitethernet priority-tag

Displays whether 802.1p priority tagging is configured for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **priority-tag**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Description Use this command to display whether AMPP port-profiling is configured for the specified interface.

Defaults This command has no default configurations.

Description Use this command to display whether AMPP port-profiling is configured for the specified interface.

Command Modes Privileged EXEC mode

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 priority-tag
interface GigabitEthernet 1/0/8
 priority-tag
!
```

See Also **priority-tag**

show running-config interface gigabitethernet qos

Displays the quality of service (QoS) configured for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **qos [cos | cos-mutation | cos-traffic-class | flowcontrol [rx | tx] | trust [cos]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
cos	Displays only the cos value configured for the interface.
cos-mutation	Displays the Cos-to-CoS mutation QoS map configured for the interface.
cos-traffic-class	Displays the CoS-to-Traffic Class QoS Map configured for the interface.
flowcontrol	Displays the activation status of QoS flow control on the interface.
rx	Displays the activation status of the receive portion of flow control for the interface.
tx	Displays the activation status of the transmit portion of flow control for the interface.
trust cos	Displays the configured QoS trust mode for the interface.

Defaults By default, this command displays the full QoS configuration for the interface.

Command Modes Privileged EXEC mode

Description Use this command to display the QoS configuration for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples None

See Also **qos cos, qos cos-mutation, qos cos-traffic-class, qos flowcontrol tx, qos trust cos, show qos flowcontrol interface, show qos interface, show qos queue interface, show qos rcv-queue interface**

show running-config interface gigabitethernet rmon

Displays the Remote Monitoring protocol (RMON) configuration for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **rmon [collection [history** *index* **| stats** *index*]]

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
collection	Displays configuration information for RMON collections.
history	Displays configuration information for RMON history collections.
stats	Displays configuration information for RMON statistics collections.
index	Specifies a valid RMON collection control index value.

Defaults By default, this command displays all RMON collection configuration information.

Command Modes Privileged EXEC mode

Description Use this command to display the RMON configuration for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 rmon collection
interface GigabitEthernet 1/0/8
 rmon collection stats 10 owner RMON_SNMP
 rmon collection history 10 owner RMON_SNMP
!
```

See Also **rmon collection history, rmon collection stats**

show running-config interface gigabitethernet sflow

Displays the sFlow configuration for a 1 GB Ethernet interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **sflow [enable | polling-interval | sample-rate]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
enable	Displays whether sFlow is enabled for the port.
polling-interval	Displays the configured maximum number of seconds between successive samples of counters to be sent to the collector.
sample-rate	Displays the number of packets that are skipped before the next sample is taken for the interface.

Defaults By default, this command displays all sFlow configuration information for the port.

Command Modes Privileged EXEC mode

Description Use this command to display the sFlow configuration for the specified interface.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 sflow
interface GigabitEthernet 1/0/8
 sflow enable
 sflow polling-interval 10
 sflow sample-rate 100
!
```

See Also **sflow enable (interface version), sflow polling-interval (interface version), sflow sample-rate (interface version)**

show running-config interface gigabitethernet shutdown

Displays whether a 1 GB Ethernet interface is enabled.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **shutdown**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default behavior.

Command Modes Privileged EXEC mode

Description Use this command to display whether the specified 1 GB Ethernet interface is enabled.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 shutdown
interface GigabitEthernet 1/0/8
 no shutdown
!
```

See Also **shutdown**

show running-config interface gigabitethernet switchport

Displays the configured switching characteristics for the 1 GB Ethernet layer 2 interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **switchport [access [vlan] | mode | trunk [allowed [vlan] |native-vlan | tag [native-vlan]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
access	Displays whether the layer 2 interface is configured as access.
access vlan	Displays whether the specific VLAN on the layer 2 interface is configured as access.
mode	Displays whether the layer 2 interface is configured for access, trunk or converged.
trunk	Displays whether the layer 2 interface is configured for trunk.
trunk allowed	Displays the configuration settings that determine the VLANs that will transmit and receive through the layer 2 interface.
trunk allowed vlan	Displays the configuration settings for a specific VLAN.
trunk allowed native-vlan	Displays the configured native VLAN characteristics of the layer 2 trunk interface for classifying untagged traffic.
trunk tag	Displays whether tagging is enabled.
tag native-vlan	

Defaults By default, this command displays all configured layer 2 switching characteristics for the port.

Command Modes Privileged EXEC mode

Description Use this command to display configured switching characteristics for the port.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 switchport
interface GigabitEthernet 1/0/8
 switchport
 switchport mode access
 switchport access vlan 1
!
```

See Also **switchport, switchport access, switchport mode, switchport trunk allowed vlan**

show running-config interface gigabitethernet vlan

Displays information about VLAN classification groups for the 1 GB Ethernet layer 2 interface.

Synopsis **show running-config interface gigabitethernet** *rbridge-id* | *slot* | *port* **vlan [classifier [activate [group]]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
classifier	Displays VLAN classifier commands for the Layer 2 interface.
activate	Displays VLAN classifier activate commands for the Layer 2 interface.
group	Displays VLAN classifier activate group commands for the Layer 2 interface.

Defaults This command has no default behavior.

Command Modes Privileged EXEC mode

Description Use this command to display VLAN classifier commands executed for the port.

Usage Guidelines This command can be used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 vlan
interface GigabitEthernet 1/0/8
 vlan classifier activate group 1 vlan 2
!
```

See Also **show vlan classifier, switchport, vlan classifier activate group, vlan classifier group, vlan classifier rule**

show running-config interface management

Displays the management interface configuration.

Synopsis **show running-config interface management** [*rbridge-id/* | *port]* [*ip*] **access group**

Operands

rbridge-id/ | *port*	Specifies the management interface to be displayed as the *rbridge-id* followed by a slash (/) and the port number.
port	On standalone platforms, the port number for the management port is always 0. On a modular switches with two redundant management modules, can configure two management ports, 1 and 2.
ip	Displays the IP addresses configured for the management interface.Use one of the following options to display selected addresses only.
access-group	Displays the access lists (ACLs) configured on the management interface.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to show configuration attributes for an AAA server.

Usage Guidelines None

Examples Example of displaying the authentication mode:

```
switch# show running-config interface Management 2/2
interface Management 2/2
  .
  ip access-group extdACL5
  .
```

See Also **show running-config ip access-list, interface management, ip access-list**

show running-config interface port-channel

Displays the status of port-channel interfaces.

Synopsis **show running-config interface port-channel** [*number*]

Operands *number* Specifies a valid port-channel number.

Defaults By default. this command displays the configuration of all port channel interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of port channel interfaces.

Usage Guidelines None

Examples To display configuration information about all port channel interfaces on a Brocade VDX 6710 switch:

```
switch# show running-config interface port-channel
interface Port-channel 1
 description 1
 shutdown
!
interface Port-channel 2
 switchport
 switchport mode access
 switchport access vlan 1
 shutdown
!
interface Port-channel 3
 shutdown
!
```

See Also **interface**

show running-config interface tengigabitethernet

Displays the status of 10 GB Ethernet interfaces.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id* | *slot* | *port*]

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults By default. this command displays the configuration of all 10 GB interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of 10 GB Ethernet interfaces.

Usage Guidelines None

Examples To display configuration information about all 10GB Ethernet interfaces on a Brocade VDX 6710 switch:

```
switch# show running-config interface tengigabitethernet
interface TenGigabitEthernet 22/0/49
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 22/0/50
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 22/0/51
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 22/0/52
 fabric isl enable
 fabric trunk enable
 sflow enable
 no shutdown
!
interface TenGigabitEthernet 22/0/53
 fabric isl enable
 fabric trunk enable
 sflow enable
 shutdown
!
interface TenGigabitEthernet 22/0/54
 fabric isl enable
 fabric trunk enable
!
```

See Also interface

show running-config interface tengigabitethernet bpdu-drop

Displays the BPDU drop status of a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **bpdu-drop [enable]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
enable	Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display information about dropped BPDUs on the specified Ethernet interface.

Usage Guidelines STP, RSTP, or MSTP must be configured.

Brocade Network OS v3.0.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples To display BPDU drop status information for a specific 1 GB Ethernet port:

```
switch# show running-config interface gigabitethernet 1/0/49 bpdu-drop
```

See Also interface

show running-config interface tengigabitethernet cee

Displays whether the default CEE map has been applied to a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **cee**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to determine whether the default CEE map has been applied to an interface.

Usage Guidelines This command does not apply to ISL ports.

Examples None

See Also **cee**

show running-config interface tengigabitethernet channel-group

Displays channel group configuration information for an interface participating in link aggregation.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **channel-group [mode | type]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
mode	Displays the mode of link aggregation (active, passive, or on).
type	Displays the type of link aggregation (802.3ad standard-based LAG, or Brocade proprietary hardware-based trunking).

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display information about the channel group configuration of the specified Ethernet interface.

Usage Guidelines This command is relevant only to interfaces configured as part of a LAG.

Examples None

See Also **channel-group**

show running-config interface tengigabitethernet description

Displays the description string associated with a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **description**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display the description string associated with the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/52 description
interface GigabitEthernet 1/0/52
 description Connects to storage device 1
!
```

See Also **description (interfaces), interface**

show running-config interface tengigabitethernet dot1x

Displays IEEE 802.1x port-based access control configuration information for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **dot1x [authentication | port-control | protocol-version | quiet-period | reauthMax | reauthentication | timeout [re-authperiod | server-timeout | supp-timeout | tx-period]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
authentication	Indicates whether 802.1x port-based access control is enabled on the interface.
port-control	Displays the status of port authorization: auto (authentication on the port is enabled), forced authorize, or force unauthorize.
protocol-version	Displays the version number of the dot1x protocol.
quiet-period	Displays the number of seconds between a failed authentication and the next authentication retry.
reauthMax	Displays the maximum number of reauthentication attempts before the port goes into the reauthorized state.
reauthentication	Indicates whether reauthentication is enabled on a port.
timeout	Displays 802.1x timeout values.
re-authperiod	Displays the reauthentication interval in seconds.
server-timeout	Displays the number of seconds the switch waits for a response from the authentication server.
supp-timeout	Displays the number of seconds that the switch waits for a response to the Extensible Authentication Protocol (EAP) frame.
tx-period	Displays the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before retransmitting the request

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display configuration information for an interface configured for IEEE 802.1x port-based access control.

Usage Guidelines This command has no usage guidelines.

Examples To display the 802.1x port-based authentication configuration for a 1 GB Ethernet interface:

```
switch# show running-config interface gigabitethernet 1/0/49 dot1x
interface GigabitEthernet 1/0/49
 dot1x authentication
 dot1x port-control auto
 dot1x quiet-period 120
 dot1x reauthMax 5
 dot1x reauthentication
 dot1x timeout server-timeout 60
!
```

See Also dot1x authentication, dot1x port-control, dot1x quiet-period, dot1x reauthentication, dot1x reauthMax, dot1x timeout re-authperiod, dot1x timeout server-timeout, dot1x timeout supp-timeout, dot1x timeout tx-period

show running-config interface tengigabitethernet fabric

Displays fabric protocol configuration parameters for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **fabric [isl [enable] | trunk [enable]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
isl [**enable**]	Indicates only the administration and operational state the interswitch link (ISL).
trunk [**enable**]	Indicates only whether trunking is enabled on the port.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display ISL and trunking status for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49
fabric             interface TenGigabitEthernet 1/0/49
 fabric isl enable
 fabric trunk enable
!
```

See Also **fabric isl enable, fabric trunk enable**

show running-config interface tengigabitethernet fcoeport

Displays whether a 10 GB Ethernet interface is configured as an FCoE port.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **fcoeport**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to determine whether a port is configured for FCoE.

Usage Guidelines This command has no usage guidelines.

Examples None

See Also **fcoe, fcoeport**

show running-config interface tengigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **lacp [timeout]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
timeout	Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display LACP settings for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples None

See Also **lacp timeout**

show running-config interface tengigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **lldp [dcbx-version | disable | iscsi-priority | profile]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
dcbx-version	Displays the configured version of the Data Center Bridging Exchange (DCBX) protocol.
disable	Indicates whether LLDP is disabled on the interface.
iscsi-priority	Displays the configured priority that will be advertized in the DCBX iSCSI TLV.
profile	Displays the LLDP profile configured on the interface.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display Link Layer Discovery Protocol (LLDP) configuration information for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples None

See Also **lldp dcbx-version, lldp disable, lldp iscsi-priority, lldp profile**

show running-config interface tengigabitethernet mac

Displays configured MAC parameters for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **mac [access-group]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
access-group	Displays MAC ACLs configured for the specified interface.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display configured MAC parameters for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples None

See Also **mac access-group**

show running-config interface tengigabitethernet mtu

Displays the configured MTU for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **mtu**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display the configured MTU for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/49 mtu
interface GigabitEthernet 1/0/49
 mtu 2500
!
```

See Also **ip mtu**

show running-config interface tengigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **port-profile-port**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display whether AMPP port-profiling is configured for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/50
port-profile-port
interface GigabitEthernet 1/0/50
 port-profile-port
!
```

See Also **port-profile-port**

show running-config interface tengigabitethernet priority-tag

Displays whether 802.1p priority tagging is configured for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **priority-tag**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display whether 802.1p priority tagging is configured for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/51 priority-tag
interface GigabitEthernet 1/0/51
 priority-tag
!
```

See Also **priority-tag**

show running-config interface tengigabitethernet qos

Displays the quality of service (QoS) configured for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **qos [cos | cos-mutation | cos-traffic-class | flowcontrol [rx | tx] | trust [cos]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
cos	Displays only the cos value configured for the interface.
cos-mutation	Displays the Cos-to-CoS mutation QoS map configured for the interface.
cos-traffic-class	Displays the CoS-to-Traffic Class QoS Map configured for the interface.
flowcontrol	Displays the activation status of QoS flow control on the interface.
rx	Displays the activation status of the receive portion of flow control for the interface.
tx	Displays the activation status of the transmit portion of flow control for the interface.
trust cos	Displays the configured QoS trust mode for the interface.

Defaults By default, this command displays the full QoS configuration for the interface.

Command Modes Privileged EXEC mode

Description Use this command to display the QoS configuration for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples None

See Also **qos cos, qos cos-mutation, qos cos-traffic-class, qos flowcontrol tx, qos trust cos, show qos flowcontrol interface, show qos interface, show qos queue interface, show qos rcv-queue interface**

show running-config interface tengigabitethernet rmon

Displays the Remote Monitoring protocol (RMON) configuration for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **rmon [collection [history** *index* **| stats** *index***]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
collection	Displays configuration information for RMON collections.
history	Displays configuration information for RMON history collections.
stats	Displays configuration information for RMON statistics collections.
index	Specifies a valid RMON collection control index value.

Defaults By default, this command displays all RMON collection configuration information.

Command Modes Privileged EXEC mode

Description Use this command to display the RMON configuration for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/49 rmon collection
interface GigabitEthernet 1/0/49
 rmon collection stats 10 owner RMON_SNMP
 rmon collection history 10 owner RMON_SNMP
!
```

See Also **rmon collection history, rmon collection stats**

show running-config interface tengigabitethernet sflow

Displays the sFlow configuration for a 10 GB Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **sflow [enable | polling-interval | sample-rate]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
enable	Displays whether sFlow is enabled for the port.
polling-interval	Displays the configured maximum number of seconds between successive samples of counters to be sent to the collector.
sample-rate	Displays the number of packets that are skipped before the next sample is taken for the interface.

Defaults By default, this command displays all sFlow configuration information for the port.

Command Modes Privileged EXEC mode

Description Use this command to display the sFlow configuration for the specified interface.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/53 sflow
interface GigabitEthernet 1/0/53
 sflow enable
 sflow polling-interval 10
 sflow sample-rate 100
!
```

See Also **sflow enable (interface version), sflow polling-interval (interface version), sflow sample-rate (interface version)**

show running-config interface tengigabitethernet shutdown

Displays whether a 10 GB Ethernet interface is enabled.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **shutdown**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults This command has no default behavior.

Command Modes Privileged EXEC mode

Description Use this command to display whether the specified 10 GB Ethernet interface is enabled.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/52 shutdown
interface GigabitEthernet 1/0/52
 no shutdown
!
```

See Also **shutdown**

show running-config interface tengigabitethernet switchport

Displays the configured switching characteristics for the 10 GB Ethernet layer 2 interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **switchport [access [vlan] | mode | trunk [allowed [vlan] |native-vlan | tag [native-vlan]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
access	Displays whether the layer 2 interface is configured as access.
access vlan	Displays whether the specific VLAN on the layer 2 interface is configured as access.
mode	Displays whether the layer 2 interface is configured for access, trunk or converged.
trunk	Displays whether the layer 2 interface is configured for trunk.
trunk allowed	Displays the configuration settings that determine the VLANs that will transmit and receive through the layer 2 interface.
trunk allowed vlan	Displays the configuration settings for a specific VLAN.
trunk allowed native-vlan	Displays the configured native VLAN characteristics of the layer 2 trunk interface for classifying untagged traffic.
trunk tag	Displays whether tagging is enabled.
tag native-vlan	

Defaults By default, this command displays all configured layer 2 switching characteristics for the port.

Command Modes Privileged EXEC mode

Description Use this command to display configured switching characteristics for the port.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 switchport
interface GigabitEthernet 1/0/49
 switchport
 switchport mode access
 switchport access vlan 1
!
```

See Also **switchport, switchport access, switchport mode, switchport trunk allowed vlan**

show running-config interface tengigabitethernet vlan

Displays information about VLAN classification groups for 10 GB Ethernet layer 2 interface.

Synopsis **show running-config interface tengigabitethernet** *rbridge-id* | *slot* | *port* **vlan [classifier [activate [group]]]**

Operands

rbridge-id	Specifies a switch by its RBridge-ID.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
classifier	Displays VLAN classifier commands for the Layer 2 interface.
activate	Displays VLAN classifier activate commands for the Layer 2 interface.
group	Displays VLAN classifier activate group commands for the Layer 2 interface.

Defaults This command has no default behavior.

Command Modes Privileged EXEC mode

Description Use this command to display VLAN classifier commands executed for the port.

Usage Guidelines This command has no usage guidelines.

Examples

```
switch# show running-config interface gigabitethernet 1/0/49 vlan
interface GigabitEthernet 1/0/49
 vlan classifier activate group 1 vlan 2
!
```

See Also **show vlan classifier, switchport, vlan classifier activate group, vlan classifier group, vlan classifier rule**

show running-config interface vlan

Displays the status of VLAN interfaces.

Synopsis **show running-config interface vlan** [*vlan-id*] [**arp-ageing-timeout | description | ip | mac access-group | shutdown | spanning-tree**]

Operands

vlan-id	Specifies a VLAN by its VLAN ID.
arp-ageing-timeout	Displays the configured interface timeout value in minutes for the Address Resolution Protocol (ARP) for VLANs.
description	Displays the description text entered for each VLAN or for the specified VLAN.
ip	Displays IP configuration information for VLANs.
mac access-group	Displays MAC ACLs configured for VLANs.
shutdown	Specifies whether the VLAN interface is enabled.
spanning-tree	Displays spanning tree configuration information for VLANs.

Defaults By default. this command displays the configuration of all VLAN interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of VLAN interfaces.

Usage Guidelines None

Examples None

See Also **interface**, **show running-config interface vlan ip**

show running-config interface vlan ip

Displays the IP configuration of VLAN interfaces.

Synopsis **show running-config interface vlan** [*vlan-id*] **ip [address | igmp [last-member-query-interval | query-interval | query-max-response-time | snooping [enable | fast-leave | mrouter | mrouter-timeout | querier] | static-group** *static-group-address*] **| mtu | proxy-arp]**

Operands

vlan-id	Specifies a VLAN by its VLAN ID.
address	Displays the IP address configured for VLANs.
igmp	Displays whether the Internet Group Management Protocol (IGMP) is enabled for VLANs.
last-member-query-interval	Displays the amount of time in seconds that the IGMP router waits to receive a response to a group query message.
query-interval	Displays the amount of time in seconds between IGMP query messages sent by the switch.
query-max-response-time	Displays the configured maximum response time in seconds for IGMP queries.
snooping	Displays IGMP snooping configuration information for VLANs.
enable	Indicates whether IGMP snooping is enabled for specified VLANs.
fast-leave	Indicates if snooping fast leave is enabled.
mrouter	Displays multicast router port information for the VLAN.
mrouter-timeout	Displays the configured multicast router IGMP timeout value in seconds.
querier	Indicates if IGMP snooping querier is configured.
static-group	Displays configured static group membership entries.
static-group-address	Specifies an IPv4 address to return static group information about.
mtu	Displays the MTU configured for each VLAN.
proxy-arp	Indicates whether a proxy ARP is configured for VLAN interfaces.

Defaults By default, this command displays configured information for all VLAN interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the IP configuration for VLAN interfaces.

Usage Guidelines None

Examples To display IP configuration information for all configured VLANs:

```
switch# show running-config interface vlan ip
interface Vlan 1
 !
interface Vlan 2
 ip igmp query-interval 200
 ip igmp query-max-response-time 15
 ip igmp snooping enable
!
```

See Also show running-config interface management, interface management, ip access-list

show running-config ip access-list

Displays the configuration for the IP ACL and its configured rules.

Synopsis **show running-config ip access-list** [**ip** | **ipv6**]

Operands

ip | **ipv6**	Specifies the IP type. An ACL can contain rules for only one version of IP (either IPv4 or IPv6).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the ACL parameters.

Usage Guidelines None

Examples The following example shows the display of a configured ACL with rules.

```
switch# show running-config ip access-list
ip access-list standard stdACL3
  seq 5 permit host 10.20.33.4
  seq 7 permit any

ip access-list extended extdACL5
  seq 5 deny tcp host 10.24.26.145 any eq 23
  seq 7 deny tcp any any eq 80
  seq 10 deny udp any any range 10 25
  seq 15 permit tcp any

ip access-list extended extdACLwithNoRules
```

See Also **show running-config interface management, interface management, ip access-list**

show running-config ip dns

Displays the domain name service (DNS) parameters.

Synopsis **show running-config ip dns**

Operands None

Description Use this command to display the configured DNS parameters. The DNS parameters are the domain name and the name server IP address for primary and secondary name servers.

Command Modes Privileged EXEC mode

Defaults None

Usage Guidelines None

Examples To display the configured DNS parameters:

```
switch# show running-config ip dns
ip dns domain-name brocade.com
ip dns name-server 10.70.20.1
ip dns name-server 10.70.20.10
```

See Also ip dns

show running-config ip igmp

Displays IGMP configuration information.

Synopsis **show running-config ip igmp** [**snooping** [**enable**]]

Operands

snooping	Displays IGMP snooping configuration information.
enable	Displays whether IGMP snooping is enabled.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display IGMP snooping configuration information.

Usage Guidelines None

Examples To display IGMP configuration information:

```
switch# show running-config ip igmp
```

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

show running-config ip route

Displays routing information.

Synopsis **show running-config ip route [next-hop | next-hop-enable-default | next-hop-recursion | routing-table]**

Operands

next-hop	Displays the routing protocol configured for resolving the next hop.
next-hop-enable-default	Specifies enabling of next hop resolution to default.
next-hop-recursion	Specifies next hop recursion.
routing-table	Displays a specific route to a specific destination.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display routing information.

Usage Guidelines None

Examples None

See Also None

show running-config ldap-server

Displays the Lightweight Directory Access Protocol (LDAP) server configuration.

Synopsis **show running-config ldap-server** [**host** *ipaddr*|*host-name*]

Operands

host *ipaddr*	Specifies the IP address of the LDAP server.
host-name	Specifies the host name of the LDAP server

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the current LDAP server configuration.

Usage Guidelines This command does not display attributes holding default values.

Examples

```
To displays the current LDAP server configuration:
switch# show running-config ldap-server host 10.24.65.6
ldap-server host 10.24.65.6
 port        3890
 domain      security.brocade.com
 retries     3
!
```

See Also **certutil import ldapca**, **ldap-server host**, **ldap-server maprole**

show running-config line

Displays command-line session configuration information.

Synopsis **show running-config line** [**vty** [**exec-timeout**]]

Operands

vty	Displays the terminal type.
exec-timeout	Displays the configured idle time in minutes before the command-line session automatically logs off.

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display configuration information about command-line sessions.

Usage Guidelines None

Examples None

See Also **interface**

show running-config logging

Displays the log configuration

Synopsis **show running-config logging**

Operands None

Defaults None.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of the logging facilities on the local switch.

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

Examples To display the logging facilities configured on the local switch:

```
switch# show running-config logging
logging rbridge-id 1
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
```

See Also show running-config logging auditlog class, show running-config logging, show running-config logging syslog-server

show running-config logging auditlog class

Displays the severity level configured for the audit log class.

Synopsis **show running-config logging auditlog class**

Operands None

Defaults Displays the information for the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the enabled audit log class.

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

This command is not supported on the standby management module.

Examples To display audit log classes enabled on the switch:

```
switch# show running-config logging auditlog class
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
```

See Also clear logging raslog, clear logging auditlog

show running-config logging raslog

Displays the severity level configured for the RASlog console.

Synopsis **show running-config logging rbridge-id** *rbridge-id* **raslog**

Operands **rbridge-id** *rbridge-id* Executes the command on the specified switch.

Defaults Displays the RASlog console configuration.

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 This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples To display the severity level configured for the RASlog console:

```
switch# show running-config logging rbridge-id 2 raslog
logging rbridgeid 2
raslog console INFO
!
```

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

show running-config logging syslog-facility

Displays the syslog facility log level.

Synopsis **show running-config logging syslog-facility** [**local**]

Operands **local** Displays the local syslog facility level.

Defaults Displays the local configuration.

Command Modes Privileged EXEC mode

Description Use this command to display the local syslog facility log level.

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

This command is not supported on the standby management module.

Examples To display the syslog daemon IP addresses configured on a switch:

```
switch# show running-config logging syslog-facility
logging syslog-facility local LOG_LOCAL7
```

See Also **logging syslog-server, show running-config logging syslog-server**

show running-config logging syslog-server

Displays the syslog server configuration.

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 This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples To display the syslog daemon IP addresses configured on a switch:

```
switch# show running-config logging syslog-server
logging syslog-server 10.17.17.203
 secure port 6514
!
logging syslog-server 10.17.17.204
```

See Also **logging syslog-server**

show running-config monitor

Displays configuration information about the monitor session.

Synopsis **show running-config monitor** {**session** *session_number* {**description**}}

Operands **session** *session_number*
The session number to display.

description Displays the session's description.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configuration information about the monitor session.

Usage Guidelines None

Examples
```
switch# show running-config monitor
monitor session 22
```

See Also None

show running-config ntp

Displays the Network Time Protocol (NTP) server configuration.

Synopsis **show running-config ntp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current NTP server configuration.

Usage Guidelines None

Examples To display the configured NTP server

```
switch# show running-config ntp
ntp server 172.26.1.159
!
```

See Also **ntp server, show ntp status**

show running-config password-attributes

Displays global password attributes.

Synopsis **show running-config password-attributes**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display global password attributes.

Usage Guidelines The attributes will not be displayed when they hold default values.

Examples To display the global password attributes:

```
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 police-priority-map

Displays configured police-priority-maps.

Synopsis **show running-config class-map**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured police class-maps.

Usage Guidelines This command is only supported on VDX 8770-4, VDX 8770-8, and later models.

Examples To display configured police-priority-maps:

```
switch# configure terminal
switch(config)# do show running-config police-priority-map
police-priority-map pmap1
     conform 0 1 1 2 1 2 1 1
     exceed 3 3 3 3 4 5 6 7
```

See Also police-priority-map

show running-config policy-map

Displays the currently running policy-map configurations.

Synopsis **show running-config policy-map**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the policy-map configurations currently operating on the switch. Output includes the policy-map name, class-map name, and class-map configuration.

Usage Guidelines None

Examples To currently running policy-maps and their configuration:

```
switch# show running-config policy-map
policy-map policy_map1
 class default
  police cir 50000 cbs 500000 eir 60000 ebs 40000 set-priority prio_map1
conform-set-dscp 23 conform-set-tc 4 exceed-set-prec 2 exceed-set-tc 5
 !
!
policy-map policy_map2
 class default
  police cir 1000000 cbs 200000
```

See Also class, qos cos, show running-config class-map, show running-config policy-map, policy-map

show running-config port-profile

Displays configured AMPP port-profiles.

Synopsis **show running-config port-profile** [*name*]

Operands

name	Specifies the name of a port-profile. If no name is provided, information about all port-profiles is displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display port-profile information.

Usage Guidelines None

Examples

```
switch# show running-config port-profile
port-profile default
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk native-vlan 1
 !
!
```

See Also port-profile, show port-profile, show running-config port-profile activate, show running-config port-profile fcoe-profile, show running-config port-profile qos-profile, show running-config port-profile security-profile, show running-config port-profile static, show running-config port-profile vlan-profile

show running-config port-profile activate

Displays activated AMPP port-profiles.

Synopsis **show running-config port-profile** [*name*] **activate**

Operands

name	Specifies the name of a port-profile. If no name is provided, information about all activated port-profiles is displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display port profiles that are activated. These port profiles are available for association with MAC addresses.

Usage Guidelines None

Examples None

See Also show running-config port-profile, port-profile

show running-config port-profile fcoe-profile

Displays the configured FCOE subprofile.

Synopsis **show running-config port-profile** [*name*] **fcoe-profile [fcoeport [default]]**

Operands

name	Specifies the name of a port-profile. If no name is provided, information about all port-profiles with the FCOE profile applied is displayed.
fcoeport [**default**]	Specifies an FCOE map name. The only map name supported currently is "default."

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about FCOE subprofiles.

Usage Guidelines None

Examples None

See Also fcoe, fcoe-profile (AMPP), port-profile, show running-config port-profile

show running-config port-profile qos-profile

Displays the configured Quality-of-Service (QoS) subprofile.

Synopsis **show running-config port-profile** [*name*] **qos-profile [cee [name] | qos [cos cos| cos-mutation** *name*| **cos-traffic-class** *name* | **flowcontrol [pfc | rx | tx] | trust [cos]]**

Operands

name	Specifies the name of a port-profile. If no name is provided, information about all port-profiles with the QoS subprofile applied is displayed.
cee [*name*]	The configured QoS CEE map.
qos	**The QoS profile.**
cos *cos*	*The configured default class of service (CoS).*
cos-mutation *name*	The applied Cos-to-Cos mutation map.
cos-traffic-class *name*	The applied Cos-to-Traffic class map.
flowcontrol	**The configured IEEE 802.3x flow control.**
pfc	Whether priority-based flow control (PFC) is enabled.
rx	Whether Pause reception is enabled.
tx	Whether Pause generation is enabled.
trust	The configured QoS trust configuration.
cos	Whether the L2 CoS field in incoming packets is configured as trusted for deriving the internal traffic class.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display QoS subprofiles.

Usage Guidelines None

Examples None

See Also port-profile, qos cos, qos cos-mutation, qos map cos-traffic-class, qos flowcontrol tx, qos flowcontrol pfc, qos-profile (AMPP), show running-config port-profile,

show running-config port-profile security-profile

Displays security subprofiles.

Synopsis **show running-config port-profile** [*name*] **security-profile** [**mac** [**access-group** [*acl-name* | **in**]]]

Operands

name	Specifies the name of a port-profile. If no name is provided, information about all port-profiles with the security subprofile applied is displayed.
mac	The configured MAC parameters.
access-group	The applied ACL.
acl-name	*Specifies an ACL.*
in	**Ingress direction.**

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display security subprofiles.

Usage Guidelines None

Examples None

See Also mac access-group, port-profile, port-profile-port, security-profile (AMPP), show running-config port-profile

show running-config port-profile static

Displays statically associated VM MAC addresses.

Synopsis **show running-config port-profile** [*name*] **static** [*mac-address*]

Operands

name	Specifies the name of a port-profile. If no name is provided, information about all port-profiles associated with VM MAC addresses is displayed.
mac-address	Displays the port-profile associated with a specific MAC address.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display VM MAC addresses and the port profiles with which they are statically associated.

Usage Guidelines None

Examples None

See Also show running-config port-profile, port-profile

show running-config port-profile vlan-profile

Displays information about VLAN subprofiles.

Synopsis **show running-config port-profile** [*name*] **vlan-profile** [**switchport** [**access** [**vlan** [*vlan-interface-number*]]| **mode** [**access** | **trunk**] | **trunk** [**allowed** [**vlan** [**add** [*vlan-id*]| **all** | **except** *vlan-id* | **none** | **remove** [*vlan-id*]] | **native-vlan** *vlan-id*]]]

Operands

name Specifies the name of a port-profile. If no name is provided, information about all port-profiles with a VLAN subprofile applied is displayed.

switchport The configured switching characteristics of the L2 interfaces.

access VLAN interfaces for which access is configured for the VLAN profile mode.

vlan *vlan-interface-number*
Specific VLAN interfaces configured for access.

mode Configured mode of the L2 interface.

access L2 interfaces configured for access mode.

trunk L2 interfaces configured for trunk mode.

trunk L2 interfaces configured for trunk mode.

allowed VLANs that are configured to transmit and receive through the Layer2 interface.

vlan add [*vlan-interface-number*]
Specific VLANs that are allowed to transmit and receive through the L2 interface.

vlan all Whether all VLANs are allowed to transmit and receive through the L2 interface.

vlan except *vlan-interface-number*
VLANs excepted from transmitting and receiving through the L2 interface.

vlan none Whether no VLANs are allowed to transmit and receive through the Layer2 interface.

vlan remove [*vlan-interface-number*]
Specific VLANs to be removed from those allowed to transmit and receive through the L2 interface.

native-vlan *vlan-interface-number*
Native VLANs configured to classify untagged traffic.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about configured VLAN subprofiles.

Usage Guidelines None

Examples

```
sw0# show running-config port-profile vlan-profile
port-profile default
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk native-vlan 1
 !
!
switch# show running-config port-profile vlan-profile switchport trunk
native-vlan
port-profile default
 vlan-profile
  switchport trunk native-vlan 1
 !
!
```

See Also port-profile, show running-config port-profile, switchport, switchport access, switchport mode, switchport trunk allowed vlan, vlan-profile (AMPP)

show running-configuration protocol cdp

Displays the Cisco Discovery Profile (CDP) information.

Synopsis **show running-configuration protocol cdp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about Cisco Discovery Profile (CDP).

Usage Guidelines None

Examples None

See Also None

show running-configuration protocol edge

Displays the edge loop detection (ELD) parameters.

Synopsis **show running-configuration protocol edge {hello-interval | pdu-rx-limit | shutdown-time}**

Operands

hello-interval	Displays the hello-interval-limit value.
pdu-rx-limit	Displays the bpdu-rx-limit value.
shutdown-time	Displays the shutdown-time-limit value.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about edge loop detection (ELD) parameters.

Usage Guidelines None

Examples None

See Also None

show running-configuration protocol lldp

Displays the LLDP parameters.

Synopsis **show running-configuration protocol lldp advertise** {{**dcbx-fcoe-app-tlv** | **dcbx-fcoe-logical-link-tlv** | **dcbx-iscsi-app-tlv** | **dcbx-tlv** | **dot1-tlv** | **dot3-tlv** | **optional-tlv**} | **description** | **disable** | **hello** | **iscsi-priority** | **mode** | **multiplier** | **profile** {**description**} | **system-description** | **system-name**}

Operands

advertise	Displays the Advertise TLV configuration information.
dcbx-fcoe-app-tlv	Displays the IEEE Data Center Bridging eXchange FCoE Application TLV information.
dcbx-fcoe-logical-link-tlv	Displays the IEEE Data Center Bridging eXchange FCoE Logical Link TLV information.
dcbx-iscsi-app-tlv	Displays the IEEE Data Center Bridging eXchange iSCSI Application TLV information.
dcbx-tlv	Displays the IEEE Data Center Bridging eXchange TLV information.
dot1-tlv	Displays the IEEE 802.1 Organizationally Specific TLV information.
dot3-tlv	Displays the IEEE 802.3 Organizationally Specific TLV information.
optional-tlv	Displays the Optional TLVs information.
description	Displays the User description
disable	Displays the Disable LLDP
hello	Displays the Hello Transmit interval.
iscsi-priority	Displays the Ethernet priority to advertise for iSCSI
mode	Displays the LLDP mode.
multiplier	Displays the Timeout Multiplier
profile description	Displays the LLDP Profile table and description.
system-description	Displays the System Description.
system-name	Displays the System Name

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the LLDP parameters.

Usage Guidelines None

Examples None

See Also None

show running-config radius-server

Displays the local switch configuration for the RADIUS server from the configuration database.

Synopsis **show running-config radius-server host** {*ipaddress* | *hostname*}

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.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display RADIUS server configuration parameters on the local switch..

Usage Guidelines None

Examples

```
switch# show running-config radius-server host 10.38.37.180
radius-server host 10.38.37.180
protocol   pap
key          changedsec
timeout    3
```

See Also radius-server, show running-config tacacs-server, tacacs-server

show running-config rbridge-id

Displays configuration for the Rbridge ID.

Synopsis **show running-config rbridge-id** *rbridge-id*

Operands **rbridge-id** *rbridge-id* Specifies the Rbridge ID for which to display the attribute.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the Rbridge ID configuration parameters.

Usage Guidelines None

Examples

```
switch# show running-config rbridge-id 2
rbridge-id 2
 interface-nodespecific ns-vlan 10
 interface-nodespecific ns-ethernet 100
 fabric vlag 10 load-balance src-dst-mac-vid
 fabric vlag 20 load-balance dst-mac-vid
 no protocol vrrp
!
```

See Also **show fabric vlag-load-balance**

show running-config rbridge-id linecard

Displays the interface module (line card) configuration.

Synopsis **show running-config rbridge-id** *rbridge-id* **linecard**

Operands **rbridge-id** *rbridge-id* Specifies the Rbridge ID for which to display the attribute.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display slot configuration for the interface modules in the chassis.

Usage Guidelines This command must be executed in the current rbridge-id context.

Examples To display the interface module configuration for the local switch:

```
switch# show running-config rbridge-id 1 linecard
rbridge-id 1
 linecard 1 LC48x10G
 linecard 2 LC48x10G
 linecard 3 LC12x40G
 linecard 4 LC48x10G
```

See Also linecard

show running-config rmon

Displays Remote Monitor configuration information.

Synopsis **show running-config rmon** [**alarm** | **event**]

Operands

alarm	Displays the Remote Monitor alarm configuration.
event	Displays the Remote Monitor event configuration

Defaults This command has no default configurations.

Command Modes Privileged EXEC mode

Description Use this command to display Remote Monitor configuration information.

Usage Guidelines None

Examples None

See Also **rmon alarm, rmon event**

show running-config role

Displays the configured roles .

Synopsis **show running-config role** [**name** *role_name*]

Operands **name** *role_name* Specifies role assigned to the user.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the roles that have been created and their descriptions.

Usage Guidelines None

Examples To display the roles configured on the switch:

```
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 **role, rule, show running-config rule**

show running-config rule

Displays configured access rules

Synopsis **show running-config rule** [*index*] [**{action {reject | accept} | command** *command_name* **| operation {read-only | read-write} | role** *role_number* **}**]

Operands

rule	Displays all configured rules
index	Displays the rule with the specified index number. The valid range is from 1 through 512.
action {reject | accept}	Displays all rules with the specified action: accept or reject.
command *command_name*	Displays all rules for the specified comand. Type a question mark (?) to display a list of valid commands.
operation {read-only | read-write}	Displays the operation for the command.
role *role_number*	Displays all rules for the specified role.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command without operands to display rules that have been defined and associated with a particular role.

Usage Guidelines None

Examples To display the configured roles and their access rules:

```
switch# show running-config rule

rule 30 action accept operation read-write role NetworkSecurityAdmin
rule 30 command role
!
rule 31 action accept operation read-write role NetworkSecurityAdmin
rule 31 command rule
!
rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username
!
rule 33 action accept operation read-write role NetworkSecurityAdmin
rule 33 command aaa
!
rule 34 action accept operation read-write role NetworkSecurityAdmin
rule 34 command radius-server
!
rule 35 action accept operation read-write role NetworkSecurityAdmin
rule 35 command configure
!
rule 40 action accept operation read-write role FCOEAdmin
rule 40 command "interface fcoe"
!
```

To display a single rule:

```
switch# show running-config rule 30
rule 30
 action accept operation read-write role NetworkSecurityAdmin
 command role
```

See Also role, rule, show running-config role

show running-config secpolicy

Displays the Switch Connection Control (SCC) security policy information.

Synopsis **show running-config secpolicy** {**defined-policy** | **active-policy**}

Operands

defined-policy	Displays the defined policy and its policy member set.
active-policy	Displays the active policy and its policy member set.

Defaults None

Command Modes Privileged EXEC mode

Description This command is used to show the active policy and the defined policy and its policy member set.

Usage Guidelines None

Examples To show only the defined policy:

```
switch# show running-config secpolicy defined-policy
secpolicy defined-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
```

To show only the active policy:

```
switch# show running-config secpolicy active-policy
secpolicy active-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
```

To show both the active and defined policies:

```
switch# show running-config secpolicy
secpolicy defined-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
 !
!
secpolicy active-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
```

See Also **secpolicy activate, secpolicy defined-policy**

show running-config ssh server

Displays the ssh server status in the running-config.

Synopsis **show running-config ssh server**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of ssh server in the running-config.

Usage Guidelines None

Examples

```
switch# show running-config ssh server
ssh server disable
```

See Also **ssh server shutdown, show ssh server status, ssh**

show running-config snmp-server

Shows the running configuration of the SNMP server on the switch.

Synopsis **show running-config snmp-server**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current SNMP configurations of host, community, contact, user, and location.

Usage Guidelines None

Examples The following command shows the running configuration of the SNMP server on the switch:

```
switch# show running-config snmp-server
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr “Brocade VDX Switch.”
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server host 10.17.37.107 public

snmp-server user snmp
 auth-password *
 priv-password *

snmp-server user snmpadmin2
 groupname snmpadmin
auth-password *
 priv-password *

snmp-server user snmpadmin3
 groupname snmpadmin
 auth-password *
 priv-password *

snmp-server user snmpuser2
 auth-password *
 priv-password *

snmp-server user snmpuser3
 auth md5
 auth-password *
 priv DES
 priv-password *

snmp-server user snmpadmin1 groupname snmpadmin auth-password* priv-password*
snmp-server user snmpadmin2 groupname snmpadmin auth-password* priv-password*
```

```
snmp-server user snmpadmin3 groupname snmpadmin auth-password* priv-password*
snmp-server user snmpuser1 auth-password* priv-password*
snmp-server user snmpuser2 auth-password* priv-password*
snmp-server user snmpuser3 auth-password* priv-password*
```

See Also snmp-server community, snmp-server, snmp-server contact, snmp-server location, snmp-server sys-descr, snmp-server user, snmp-server v3host

show running-config support

Displays the support parameters in the running configuration.

Synopsis **show running-config support** [**rbridge-id** *rbridge-id* [**ffdc**]]

Operands

rbridge-id *rbridge-id*	**Specifies the Rbridge ID for which to display the support parameters.**
ffdc	Displays the ffdc settings.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the support parameters in the running configuration.

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

This command is not supported on the standby management module.

Examples To display the support parameters in the running configuration:

```
switch# show running-config support
support rbridge-id 12
 ffdc
!
```

See Also **support**, show support

show running-config switch-attributes

Displays switch attributes.

Synopsis **show running-config switch-attributes** [*rbridge-id*] **{chassis-name | host-name}**

Operands

rbridge-id	**Specifies the Rbridge ID for which to display the attribute.**
chassis-name	Displays the switch chassis name.
host-name	Displays the switch host name.

Defaults Displays all switch attributes on the local switch.

The default host name is “sw0”

The default chassis name depends on the switch model.

Command Modes Privileged EXEC mode

Description Use this command to display the switch attributes.

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

This command is not supported on the standby management module.

Examples To display all attributes for the local switch:

```
switch# show running-config switch-attributes
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-config system-monitor

Displays the system monitor configuration.

Synopsis **show running-config system-monitor** [**fan** | **power** | **temp** | **cid-card** | **sfp** | **compact-flash** | **MM** | **LineCard** | **SFM**]

Operands

fan	Displays the threshold and alert setting for the FAN component.
power	Displays the threshold and alert setting for the power component.
temp	Displays the threshold for the temperature sensor component.
cid-card	Displays the threshold for the CID card component.
sfp	Displays the threshold for the small form factor pluggable (SFP) device.
compact-flash	Displays the threshold for the compact flash device.
MM	Displays the threshold for the management module.
LineCard	Displays the threshold for the line card.
SFM	Displays the threshold for the switch fabric module.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running system monitor configuration.

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

Examples

```
switch# show running-config system-monitor
system-monitor fan threshold marginal-threshold 1 down-threshold 2
system-monitor fan alert state removed action raslog
system-monitor power threshold marginal-threshold 0 down-threshold 1
system-monitor power alert state removed action raslog
system-monitor temp threshold marginal-threshold 1 down-threshold 2
system-monitor cid-card threshold marginal-threshold 1 down-threshold 0
system-monitor cid-card alert state inserted,faulty action email
system-monitor sfp alert state none action none
system-monitor compact-flash threshold marginal-threshold 1 down-threshold 0
system-monitor MM threshold marginal-threshold 1 down-threshold 0
system-monitor LineCard threshold marginal-threshold 1 down-threshold 0
system-monitor LineCard alert state removed action raslog
system-monitor SFM threshold marginal-threshold 1 down-threshold 0
```

See Also **show system monitor**, system-monitor-mail

show running-config system-monitor-mail

Displays the system monitor mail configuration.

Synopsis **show running-config system-monitor-mail** {**fru enable**}

Operands

fru	Displays FRU information.
enable	Displays the status of the FRU.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running system monitor configuration.

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

Examples None

See Also **show system monitor**, system-monitor-mail

show running-config tacacs-server

Displays the TACACS+ server configuration.

Synopsis **show running-config tacacs-server** [**host** *ipaddr* | *hostname*]

Operands

host		Identifies the TACACS+ server by host name or IP address.
	hostname	Specifies the domain name of the TACACS+ server.
	ipaddr	Specifies the IP address of the TACACS+ server (IPv4 or IPv6).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the user configuration for the TACACS+ server.

Usage Guidelines None

Examples To display the list of configured TACACS+ servers:

```
switch# show running-config tacacs-server host?
Possible completions:
  10.38.37.180  IP Address or Hostname of this TACACS+ server
  10.24.65.6    IP Address or Hostname of this TACACS+ server
  fec0:60:69bc:94:211:25ff:fec4:6010 IP Address or Hostname of this TACACS+
server
  <cr>
```

To display a single IPv4 TACACS+ server configuration:

```
switch# show running-config tacacs-server host 10.24.65.6
tacacs-server host 10.24.65.6
 key        new#tacacs*secret
 retries    100
!
```

To display a single IPv5 TACACS+ server configuration:

```
switch# show running-config tacacs-server host
fec0:60:69bc:94:211:25ff:fec4:6010
tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
key        changedsec
!
```

See Also radius-server, show running-config radius-server, tacacs-server

show running-config telnet server

Displays the telnet server status in the running-config.

Synopsis **show running-config telnet server**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of telnet server in the running-config.

Usage Guidelines None

Examples

```
switch# show running-config telnet server
telnet server disable
```

See Also **telnet server shutdown**, **show telnet server status**, **telnet**

show running-config threshold-monitor

Displays the system's threshold configuration.

Synopsis **show running-config threshold-monitor**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running system threshold configuration.

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

Examples

```
switch# show running-config threshold-monitor
threshold-monitor Cpu poll 30 retry 2 limit 60 actions raslog
threshold-monitor Memory poll 30 retry 2 limit 70 high-limit low-limit 50 actions
none

switch# show running-config threshold-monitor area IFG

Interface                          Area       Value  Status        Monitoring
                                                                      Status
---------                    ----------------  ------ -------     ------------
FortyGigabitEthernet 3/8     IFG Violation Error  30  Out of Range  Monitoring
FortyGigabitEthernet 3/9     IFG Violation Error   0  In Range      Monitoring
<All other online interfaces> IFG Violation Error   0  In Range      Monitoring
```

See Also **show system monitor**, system-monitor-mail

show running-config threshold-monitor interface

Displays the system's running interface configuration.

Synopsis **show running-config threshold-monitor interface**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running system's interface threshold configuration.

Usage Guidelines Default values are not displayed under the **show running-config threshold-monitor interface** command. Only custom values are displayed.

Examples

```
switch# do show running-config threshold-monitor interface

switch(config)# do show running-config threshold-monitor interface
threshold-monitor interface apply custom-monitoring
threshold-monitor interface pause
threshold-monitor interface policy  custom type Ethernet area
MissingTerminationCharacter threshold timebase minute high-threshold 20
low-threshold 1 buffer 5
threshold-monitor interface policy custom type Ethernet area
MissingTerminationCharacter alert above highthresh-action none lowthresh-action
none
threshold-monitor interface policy custom type Ethernet area
MissingTerminationCharacter alert below highthresh-action none lowthresh-action
none
threshold-monitor interface policy custom type Ethernet area CRCAlignErrors
threshold timebase hour high-threshold 80 low-threshold 10 buffer 35
threshold-monitor interfacepolicy  custom type Ethernet area CRCAlignErrors alert
above highthresh-action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area CRCAlignErrors alert
below highthresh-action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area SymbolErrors
threshold timebase minute high-threshold 20 low-threshold 1 buffer 5
threshold-monitor interfacepolicy custom type Ethernet area SymbolErrors alert
above highthresh-action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area SymbolErrors alert
below highthresh-action none lowthresh-action none
threshold-monitor interface policy  custom type Ethernet area IFG threshold
timebase minute high-threshold 20 low-threshold 1 buffer 5
threshold-monitor interface policy custom type Ethernet area IFG alert above
highthresh-action raslog,portfence lowthresh-action emailraslog
threshold-monitor interface policy custom type Ethernet area IFG alert below
highthresh-action none lowthresh-action none
```

See Also **show system monitor**

show running-config threshold-monitor security

Displays the system's running Security configuration.

Synopsis **show running-config threshold-monitor security**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running system's Security threshold configuration.

Usage Guidelines Default values are not displayed under the **show running-config threshold-monitor security** command. Only custom values are displayed.

Examples

```
switch# show running-config threshold-monitor security policy custom area
telnet-violation

threshold-monitor security policy custom area telnet-violation timebase hour

threshold-monitor security policy custom area telnet-violation threshold
thresh_high high-threshold 10 buffer 20

switch# show running-config threshold-monitor policy custom area login-violation

threshold-monitor securitym policy custom area login-violation alert above
highthresh_action all

threshold-monitor security apply custom
switch#
```

See Also **show system monitor**

show running-config threshold-monitor sfp

Displays the system's running SFP configuration.

Synopsis **show running-config threshold-monitor sfp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the running system's SFP threshold configuration.

Usage Guidelines Default values are not displayed under the **show running-config threshold-monitor sfp** command. Only custom values are displayed.

Examples

```
switch# do show running-config threshold-monitor sfp
threshold-monitor sfp pause
threshold-monitor sfp apply custom
threshold-monitor sfp policy custom type 1GSR area TXP threshold high-threshold
2000 low-threshold 1000 buffer 500
threshold-monitor sfp policy custom type 1GSR area TXP alert above
highthresh-action raslog lowthresh-action none
threshold-monitor sfp policy custom type 1GSR area TXP alert below
highthresh-action none lowthresh-action raslog
```

See Also **show system monitor**

show running-config username

Displays the user accounts on the switch.

Synopsis **show running-config** *username* **[[username][desc][enable][encryption-level][password][role]]**

Operands

username	The account name associated with the user. The maximum number of characters is 40.
desc	Displays the description of the user configuration.
enable	Displays the account status: enable true = enabled (default) enable false = disabled
encryption-level	Password encryption level. Values are 0 through 7. The default is 0.
password	Account password.
role	The role associated with the account.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display users and associated account parameters.

Usage Guidelines When used without operands, this command displays all user accounts on the switch.

Use the optional parameters to query the specified account details.

This command does not display the root account.

Defaults are not displayed.

Examples To display the user accounts on the switch:

```
switch# show running-config username
username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role
admin desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role
user desc User
```

To display a specific user account:

```
switch# show running-config username admin
username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role
admin desc Administrator
```

To display the enabled status for a specific user account

```
switch# show running-config username admin enable
username admin enable true
```

See Also **show users, username, unlock username**

show running-config zoning

Displays the zone configuration.

Synopsis **show running-config zoning**

Operands None

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to display the zone configuration for a Brocade VCS Fabric. The command lists both the defined and the enabled configuration

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples The following example displays the zoning configuration:

```
switch# show running-config zoning defined-configuration
zoning defined-configuration cfg cfg0
 member-zone zone_0_1
 member-zone zone_0_2
 member-zone zone_0_3
 member-zone zone_0_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg1
 member-zone zone1
 member-zone zone2
!
zoning defined-configuration cfg cfg2
 member-zone zone_2_1
 member-zone zone_2_2
 member-zone zone_2_3
 member-zone zone_2_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg4
 member-zone zone1
 member-zone zone2
!
zoning defined-configuration zone zone0
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry alias1
 member-entry alias2
 member-entry alias3
!
zoning defined-configuration zone zone1
 member-entry 10:00:00:00:00:00:00:01
 member-entry 10:00:00:00:00:00:00:02
!
```

```
zoning defined-configuration zone zone2
 member-entry 10:00:00:00:00:00:00:03
 member-entry 10:00:00:00:00:00:00:04
!
zoning enabled-configuration cfg-name "cfg1"
zoning enabled-configuration default-zone-access allccess
zoning enabled-configuration cfg-action cfg-save
zoning enabled-configuration enabled-zone zone1
 member-entry 10:00:00:00:00:00:00:01
 member-entry 10:00:00:00:00:00:00:02
!
zoning enabled-configuration enabled-zone zone2
 member-entry 10:00:00:00:00:00:00:03
 member-entry 10:00:00:00:00:00:00:04
```

See Also show running-config zoning defined-configuration, show running-config zoning enabled-configuration

show running-config zoning defined-configuration

Displays the defined zone configuration.

Synopsis **show running-config zoning defined-configuration**

Operands None

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to display the defined zone configuration for a Brocade VCS Fabric. The command lists the zones present in each configuration, and the members of each zone.

The defined configuration is the complete set of all zone objects that have been defined in the network. Multiple zone configurations can be defined, but only one can be enabled at a time.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples The following example displays the defined zoning configuration:

```
switch# show running-config zoning defined-configuration
zoning defined-configuration cfg cfg0
 member-zone zone_0_1
 member-zone zone_0_2
 member-zone zone_0_3
 member-zone zone_0_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg1
 member-zone zone_1_1
 member-zone zone_1_2
 member-zone zone_1_3
 member-zone zone_1_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg2
 member-zone zone_2_1
 member-zone zone_2_2
 member-zone zone_2_3
 member-zone zone_2_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg4
 member-zone zone2
 member-zone zone3
!
zoning defined-configuration zone zone0
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry 11:22:33:44:55:66:77:82
 member-entry 11:22:33:44:55:66:77:83
```

```
 member-entry 11:22:33:44:55:66:77:84
!
zoning defined-configuration zone zone1
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry alias1
 member-entry alias2
 member-entry alias3
!
zoning defined-configuration zone zone2
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry 11:22:33:44:55:66:77:82
 member-entry 11:22:33:44:55:66:77:83
 member-entry 11:22:33:44:55:66:77:84
!
```

See Also show running-config zoning, show running-config zoning enabled-configuration

show running-config zoning enabled-configuration

Displays the enabled zone configuration.

Synopsis **show running-config zoning enabled-configuration {cfg-action | cfg-name | default-zone-access | enabled-zone}**

Operands

cfg-action	Displays the enabled configuration action.
cfg-name	Displays the enabled configuration name.
default-zone-access	Displays the default zone access mode.
enabled-zone	Displays the enabled zones.

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to view the enabled zone configuration.

The enabled configuration is the single zone configuration that is currently enabled in a Brocade VCS Fabric. The devices an initiator can access in the network are based on this configuration. The enabled configuration is built when a specific zone configuration is enabled and all error checking has been completed successfully.

This command displays the name of the enabled zoning configuration, configuration action, access mode, and a list of effective zones their member objects. Zone member are displayed by their WWN.

The configuration name is displayed differently depending on the presence of a pending transaction. If no transaction is pending, the configuration name alone is displayed. If a transaction is pending, the configuration name is marked with an asterisk (*). The configuration action is set to cfg-save if no transaction is pending, or to cfg-none if a transaction is pending. A CFG_MARKER flag is appended to the configuration if the enabled configuration does not exactly match the defined configuration. This scenario occurs when you have an enabled configuration and make edits to the defined-configuration, and then, instead of enabling the defined configuration, you issue the **cfg-save** command.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be executed on any RBridge in a Brocade VCS Fabric.

Examples To display the enabled zoning configuration:

```
switch# show running-config zoning enabled-configuration
zoning enabled-configuration cfg-name "cfg"
zoning enabled-configuration cfg-action cfg-none
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration effective-zone zone0
 member-entry 11:22:33:44:55:66:770
 !
 member-entry 11:22:33:44:55:66:771
 !
!
```

```
zoning enabled-configuration effective-zone zone1
 member-entry 11:22:33:44:55:66:770
 !
 member-entry 11:22:33:44:55:66:771
 !
!
zoning enabled-configuration effective-zone zone2
 member-entry 11:22:33:44:55:66:770
 !
 member-entry 11:22:33:44:55:66:771
 !
```

To display only the access mode for enabled zoning configuration:

```
switch# show running-config zoning enabled-configuration default-zone-access
zoning enabled-configuration default-zone-access allaccess
```

See Also show running-config zoning, show running-config zoning defined-configuration

show secpolicy

Displays the Switch Connection Control (SCC) security policy information.

Synopsis **show running-config secpolicy** {**defined-policy** | **active-policy**}

Operands

defined-policy	Displays the defined policy and its policy member set.
active-policy	Displays the active policy and its policy member set.

Defaults None

Command Modes Privileged EXEC mode

Description This command is used to show the active policy and the defined policy and its policy member set.

Usage Guidelines None

Examples To show only the defined policy

```
switch# show running-config secpolicy defined-policy
secpolicy defined-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
```

To show only the active policy

```
switch# show running-config secpolicy active-policy
secpolicy active-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
```

To show both active and defined policy

```
switch# show running-config secpolicy
secpolicy defined-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
 !
!
secpolicy active-policy SCC_POLICY
 member-entry 11:11:11:11:11:11:11:11
 !
 member-entry 22:22:22:22:22:22:22:22
 !
 member-entry 33:33:33:33:33:33:33:33
```

See Also **secpolicy activate**, **secpolicy defined-policy**

show sflow

Displays sFlow configuration information and statistics.

Synopsis **show sflow** [**interface** {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*}] | **all**

Operands

all	**Displays all sFlow information and statistics.**
interface	DisplayssFlow information for an Ethernet interface.
tengigabitethernet	Specifies a valid 10 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
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 The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display sFlow statistics on 10 Gbps Ethernet interface 15/0/4:

```
switch# show sflow interface tengigabitethernet 15/0/4
sFlow info for interface TenGigabitEthernet 15/0/4
-------------------------------------------------
Configured sampling rate:              32768 pkts
Actual sampling rate:                  32768 pkts
Counter polling interval:              20 secs
Samples received from hardware:        0
Port backoff-threshold :               48
```

To display sFlow statistics on 1 Gbps Ethernet interface 22/0/1:

```
switch# show sflow interface gigabitethernet 22/0/1
-------------------------------------------------
sFlow info for interface GigabitEthernet 22/0/1
Configured sampling rate:              32768 pkts
Actual sampling rate:                  32768 pkts
Counter polling interval:              20 seconds
Samples received from hardware:        0
Port backoff threshold:                48
-------------------------------------------------
```

See Also None

show sfm

Displays information about the switch fabric modules present in the chassis.

Synopsis **show sfm**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the switch fabric modules present in a modular switch. The output includes the following information:

Slot	Displays the slot number. Slots for switch fabric modules are S1 through S3 for the VDX8770-4 and S1 through S6 for VDX8770-8.
Type	Displays the interface module type. The switch fabric module type is SFM.
Description	Module description
ID	Displays the module ID. The ID for the switch fabric module is 113.
Status	Displays the status of the module as one of the following:
VACANT	The slot is empty.
POWERED-OF	The module is present in the slot but is powered off.
POWERING UP	The module is present and powering on.
LOADING	The module is present, powered on, and loading the initial configuration.
DIAG RUNNING POST1	The module is present, powered on, and running the POST (power-on self-test).
DIAG RUNNING POST2	The module is present, powered on, and running the reboot power on self tests.
INITIALIZING	The module is present, powered on, and initializing hardware components.
ENABLED	The module is on and fully enabled.
DISABLED	The module is powered on but disabled.
FAULTY	The module is faulty because an error was detected.
UNKNOWN	The module is inserted but its state cannot be determined.

Usage Guidelines None

Examples To display the switch fabric modules present in a Brocade VDX 8770-4 chassis:

```
switch# show sfm

Slot  Type         Description                ID      Status
--------------------------------------------------------------------
 S1   SFM          Switch Fabric Module       113     ENABLED#
```

```
S2   SFM          Switch Fabric Module        113     ENABLED#
S3   SFM          Switch Fabric Module        113     ENABLED
# = At least one enabled SFM in these slots is required.
```

See Also show linecard, show mm, show slots

show slots

Displays information about the modules present in the chassis.

Synopsis **show slots**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about all modules present in a modular switch. The output includes the following information:

Slot	Displays the slot number. Slots for interface modules are L1 through L4 on the Brocade VDX 8770-4, and L1 through L8 on the Brocade VDX 8770-8.
Type	Displays the module type. Valid types include the following:
MM	Management Module
SFM	Switch Fabric Module
LC48X10G	48-port 10 GbE interface module (line card)
LC48X1G	48-port 1 GbE interface module
LC12X40G	12-port 10 GbE interface module
Description	Module description
ID	Module ID
112	Management Module
113	Switch Fabric Module
114	48-port 10GbE interface module
127	12-port 10 GbE interface module
Status	Displays the status of the module as one of the following:
VACANT	The slot is empty.
POWERED-OFF	The module is present in the slot but is powered off.
POWERING UP	The module is present and powering on.
LOADING	The module is present, powered on, and loading the initial configuration.
DIAG RUNNING POST1	The module is present, powered on, and running the POST (power-on self-test). This status is not valid for the management modules.
DIAG RUNNING POST2	The module is present, powered on, and running the reboot power on self tests. This status is not valid for the management modules.
INITIALIZING	The module is present, powered on, and initializing hardware components.
ENABLED	The module is on and fully enabled.

DISABLED	The module is powered on but disabled.
FAULTY	The module is faulty because an error was detected.
UNKNOWN	The module is inserted but its state cannot be determined.

Usage Guidelines None

Examples To display the modules present in a Brocade VDX 8770-4 chassis:

```
switch# show slots

Slot  Type         Description                ID      Status
------------------------------------------------------------------------
 M1   MM           Management Module          112     ENABLED
 M2                                                    VACANT
 S1                                                    VACANT#
 S2   SFM          Switch Fabric Module       113     ENABLED#
 S3                                                    VACANT
 L1   LC48X10G     48-port 10GE card          114     ENABLED
 L2   LC48X10G     48-port 10GE card          114     ENABLED
 L3                                                    VACANT
 L4   LC48X1G      48-port 1GE card           131     ENABLED
 # = At least one enabled SFM in these slots is required.
```

See Also show linecard, show sfm

show spanning-tree

Displays all Spanning Tree Protocol information.

Synopsis **show spanning-tree pvst mst-config vlan** *vlan_id*

Operands

pvst	Spanning-tree PVST+ information.
mst-config	MSTP region configuration information.
vlan *vlan_id*	Specifies the VLAN number. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display all STP information.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Brocade Network OS v3.0.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

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. Refer to "Usage Guidelines" below.

Defaults None

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 On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

The **show spanning-tree brief** command output shows the port state as *ERR*, not *root_inc*, when root guard in effect.

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** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/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.

rbridge-id Specifies a switch by its RBridge identifier.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet Specifies a valid 1 Gbps Ethernet interface.

rbridge-id Specifies a switch by its RBridge identifier.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults None

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.

The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display information on a 10 Gbps Ethernet interface:

```
switch# show spanning-tree interface tengigabitethernet 1/0/0
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 None

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** *rbridge-id/slot/port* | **interface gigabitethernet** *rbridge-id/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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display details on a specified interface for the MSTP instance running.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

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 1/0/8 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 1/0/19 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 1/0/20 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

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** *rbridge-id/slot/port* |**interface gigabitethernet** *rbridge-id/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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface for which to display the MSTP instance information.
rbridge-id	Specifies a switch by its RBridge identifier.
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 None

Command Modes Privileged EXEC mode

Description Use this command to display information on a specified instance of the MSTP.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display information on MSTP instance 1:

```
switch# show spanning-tree mst instance 1 interface tengigabitethernet 1/0/0
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** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/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.
rbridge-id	Specifies a switch by its RBridge identifier.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies a switch by RBridge identifier.
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 None

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 The **gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples To display information for the MSTP interface:

```
switch# show spanning-tree mst interface tengigabitethernet 5/0/0
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)
IST 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
-------------------------------------------------------------------------
0            DIS   DSC  2000       128   1
```

See Also show spanning-tree brief, show spanning-tree mst brief

show ssh server status

Displays the current ssh server status.

Synopsis **show ssh server status**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of ssh server.

Usage Guidelines None

Examples

```
switch# show ssh server status
Telnet server status: Enabled
```

See Also **ssh server shutdown**, **show telnet server status**, **ssh**

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
    chassis virtual-ip 10.24.73.50/20
    no diag post enable
    linecard 2 LC48x10G
    linecard 4 LC48x10G
    class-map default
     match any
    !
    logging rbridge-id 1
     raslog console INFO
    !
    logging auditlog class SECURITY
    logging auditlog class CONFIGURATION
    logging auditlog class FIRMWARE
    logging syslog-facility local LOG_LOCAL7
    switch-attributes 1
     chassis-name VDX8770-4
     host-name sw0
    !
    support rbridge-id 1
     ffdc
    !
    snmp-server contact "Field Support."
    snmp-server location "End User Premise."
    snmp-server sys-descr "Brocade VDX Switch."
    snmp-server community ConvergedNetwork
    snmp-server community OrigEquipMfr rw
    snmp-server community "Secret C0de" rw
    snmp-server community common!
[output truncated]
```

See Also show running-config, show startup-db

show startup-db

Displays the startup database information.

Synopsis **show startup-db**

Operands Refer to the usage guidelines.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the startup database information.

Usage Guidelines Use the **show startup-db ?** command to display the list of available database entries.

Examples To display the logging configuration in the startup database:

```
switch# show startup-db logging
logging rbridge-id 1
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
```

See Also show running-config, show startup-config

show statistics access-list

Displays the statistics of an access-list status, or the statistical information on the specified ACL bound to the specified interface.

Synopsis **show statistics access-list** {**ip** | **mac**} *name* **interface** {**port-channel** *index* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **fortygigabitethernet** *slot/port* | **vlan** *vlanId* | **ve** *vlanId*} {**in** | **out**}

Operands

ip | **mac**	Specifies showing the configured rules of either a L2 or L3 ACL.
name	The “name” of the ACL assigned at creation.
port-channel *index*	Specifies the port-channel index to which the ACL is bound.
gigabitethernet *slot/port*	Specifies the gigabitethernet interface to which the ACL is bound.
tengigabitethernet *slot/port*	Specifies the ten gigabitethernet interface to which the ACL is bound.
fortygigabitethernet *slot/port*	Specifies the forty gigabitethernet interface to which the ACL is bound.
vlan *vlanId*	Specifies the VLAN interface to which the ACL is bound.
ve *vlanId*	Specifies the Virtual Ethernet interface to which the ACL is bound.
in | **out**	Specifies the ACL binding direction (ingress or egress).

Defaults None

Command Modes Privileged EXEC mode

Description This command is displays the statistics of an access-list status, or the statistical information on the specified ACL bound to the specified interface.

Usage Guidelines None

Examples None

See Also None

show statistics access-list interface

Displays the statistical information on any ACL of the type specified bound on the specified interface.

Synopsis **show statistics access-list interface** {**port-channel** *index* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **fortygigabitethernet** *slot/port* | **vlan** *vlanId* | **ve** *vlanId*} {**in** | **out**}

Operands

port-channel *index* Specifies the port-channel index to which the ACL is bound.

gigabitethernet *slot/port*
Specifies the gigabitethernet interface to which the ACL is bound.

tengigabitethernet *slot/port*
Specifies the ten gigabitethernet interface to which the ACL is bound.

fortygigabitethernet *slot/port*
Specifies the forty gigabitethernet interface to which the ACL is bound.

vlan *vlanId* Specifies the VLAN interface to which the ACL is bound.

ve *vlanId* Specifies the Virtual Ethernet interface to which the ACL is bound.

in | **out** Specifies the ACL binding direction (ingress or egress).

Defaults None

Command Modes Privileged EXEC mode

Description This command is displays the statistical information on any ACL of the type specified bound on the specified interface.

Usage Guidelines None

Examples None

See Also None

show storm-control

Displays information for traffic controlled by configured rate limits.

synopsis **show storm-control**

show storm-control broadcast [**interface** {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*]

show storm-control multicast [**interface** {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*]

show storm-control interface {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*

show storm-control unknown-unicast [**interface** {**fortygigabitethernet** | **gigabitethernet** | **tengigabitethernet**} *rbridge-id/slot/port*]

operands

show storm-control Displays all BUM-related configuration in the system.

show storm-control broadcast
Displays all BUM-related configuration in the system for the broadcast traffic type.

show storm-control multicast
Displays all BUM-related configuration in the system for the multicast traffic type.

show storm-control interface type *rbridge-id/slot/port*
Displays all BUM-related configuration in the system for the specified interface. You must specify an interface type, followed by the rbridge-id/slot/port.

show storm-control unknown-unicast
Displays all BUM-related configuration in the system for the unknown-unicast traffic type.

interface type *rbridge-id/slot/port*
Specifies an interface type, followed by the rbridge-id/slot/port, for which to display all BUM-related configuration in the system for the specified traffic type. Use this option to display information on a per-port basis.

Default None.

Command Modes Privileged EXEC mode.

Description Displays broadcast, unicast, and unknown-multicast (BUM) storm-control-related configuration for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interfaces.

Usage Guidelines None.

Examples To display storm-control information for broadcast traffic on the tengigabitethernet interface 102/4/1:

```
switch# show storm-control broadcast interface tengigabitethernet 102/4/1
Interface   Type          rate (Mbps)  conformed    violated      total
Te102/4/1   broadcast     100,000      12500000000  12500000000   25000000000
```

To display storm-control information for all traffic on the tengigabitethernet interface 102/4/1:

```
switch# show storm-control interface tengigabitethernet 102/4/1
Interface   Type             rate (Mbps)  conformed   violated    total
Te102/4/1   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/1   unknown-unicast  100,000      12500000000 12500000000 25000000000
Te102/4/1   multicast        100,000      12500000000 12500000000 25000000000
```

To display storm-control information for all traffic in the system:

```
switch# show storm-control
Interface   Type             rate (Mbps)  conformed   violated    total
Te102/4/1   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/1   unknown-unicast  100,000      12500000000 12500000000 25000000000
Te102/4/1   multicast        100,000      12500000000 12500000000 25000000000
Te102/4/2   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/3   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/4   unknown-unicast  100,000      12500000000 12500000000 25000000000
```

To display storm-control information for all broadcast traffic the system:

```
switch# show storm-control broadcast
Interface   Type             rate (Mbps)  conformed   violated    total
Te102/4/1   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/2   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/3   broadcast        100,000      12500000000 12500000000 25000000000
```

show support

Displays a list of core files on the switch.

Synopsis **show support** [**rbridge-id** {*rbridge-id* | **all**}]

Operands

rbridge-id	Executes the command on the specified switches. Valid completions for rbridge-id include the following:
rbridge-id	Specifies the ID of the routing bridge. This option is not valid in standalone mode.
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 This command is supported only on the local switch.

Pagination is not supported with this command. Use the more option to display the output one page at a time.

Examples To display the core files:

```
switch# show support
No core or FFDC data files found!
```

See Also **clear support**, copy support, **show running-config support**

show system

Displays system information.

Synopsis **show system** {**rbridge-id** *rbridge-id*}

Operands

rbridge-id	Executes the command on the specified switches.
rbridge-id	*Specifies the ID of the routing bridge.*

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display system information of hardware and software details.

Usage Guidelines None

Examples To display the system information:

```
switch# show system
Stack MAC                     : 00:05:33:4B:CC:37

  -- UNIT 0 --
Unit Name                     : sw0
Switch Status                 : Online
Hardware Rev                  : 97.4
TengigabitEthernet Port(s)    : 60
Up Time                       : up 1 day, 2:29
Current Time                  : 21:20:50 GMT
NOS Version                   :
Jumbo Capable                 : yes
Burned In MAC                 : 00:05:33:4B:CC:37
Management IP                 : 10.24.85.74
Management Port Status        : UP

  -- Power Supplies --
PS1 is faulty
PS2 is OK

  -- Fan Status --
Fan 1 is Ok
Fan 2 is Ok
Fan 3 is Ok
```

See Also show version

show system monitor

Displays the overall status for a selected switch.

Synopsis **show system monitor** {**rbridge-id** [*rbridge-id* | **all**]}

Operands

rbridge-id *rbridge-id*	Specifies a switch by RBridge identifier.
all	Reports all Rbridge information.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the overall switch status and the status of the contributors defined as part of the policy.

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

Examples

```
switch# show system monitor
** System Monitor Switch Health Report **
RBridge 128     switch status            : HEALTHY
                Time of Report           : 2012-06-19 03:18:28
                Power supplies monitor   : HEALTHY
                Temperatures monitor     : HEALTHY
                Fans monitor             : HEALTHY
                CID-Card monitor         : HEALTHY
                MM monitor               : HEALTHY
                LC monitor               : HEALTHY
                SFM monitor              : HEALTHY
                Flash monitor            : HEALTHY
rontee128#
```

See Also system-monitor-mail

show telnet server status

Displays the current telnet server status.

Synopsis **show telnet server status**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of telnet server.

Usage Guidelines None

Examples

```
switch# show telnet server status
Telnet server status: Enabled
```

See Also **telnet server shutdown, show running-config telnet server**

show users

Displays the users logged into the system.

Synopsis **show users**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display active user sessions and locked user accounts.

Usage Guidelines None

Examples To display active user sessions and locked user accounts:

```
switch# show users
**USER SESSIONS**
RBridge
ID  Username    Host IP          Device  Time logged in
2   user        10.70.4.105      vty/0   2012-05-04 01:59:35
1   root        0.0.0.0          con0    2012-05-04 01:57:23
1   user        10.70.4.105      vty/0   2012-05-07 01:57:41
1   admin       10.70.4.105      vty/2   2012-05-07 01:58:41
1   user        10.70.4.105      vty/3   2012-05-07 02:04:42
**LOCKED USERS**
RBridge
ID      username
no locked users
```

See Also **show running-config username**, **username**, **unlock username**

show vcs

Displays the Brocade VCS Fabric configuration.

Synopsis **show vcs {detail | virtual-ip}**

Operands

detail	Displays detailed information about each RBridge in the fabric.
virtual-ip	Displays the virtual IP address.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the Brocade VCS Fabric parameters (VCS ID and the switch RBridge ID) and Brocade VCS Fabric mode.

Usage Guidelines The VCS ID and switch RBridge ID are displayed only in VCS-enabled mode.

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.

Examples To display the VCS summary view:

```
switch# show vcs
Config Mode    : Local-Only
VCS ID         : 1
Total Number of Nodes           : 6
Rbridge-Id       WWN                           Management IP   Status     HostName
-----------------------------------------------------------------------------------
38               10:00:00:05:33:52:2A:82     10.17.10.38     Online          sw0
80               10:00:00:05:33:78:00:00*    10.17.11.80     Online          sw0
82               10:00:00:05:33:6F:2B:D2     10.17.10.82     Online          sw0
84               10:00:00:05:33:14:B2:70     10.17.10.84     Online          sw0
100              10:00:00:05:33:77:C9:78     10.17.11.100    Online          sw0
120             >10:00:00:05:33:4C:80:0C     10.17.10.120    Online          sw0
```

To display the VCS configuration details”:

```
switch# show vcs details
Config Mode    : Local-Only
VCS ID         : 1
Total Number of Nodes           : 6
Node :1
    Serial Number : BKN2501G00R
    Condition     : Good
    Status        : Connected to Cluster
    VCS Id        : 1
    Rbridge-Id    : 38
    Co-ordinator  : NO
    WWN           : 10:00:00:05:33:52:2A:82
    Switch MAC    : 00:05:33:52:2A:82
    FCF MAC       : 0B:20:B0:64:10:27
    Switch Type   : BR-VDX6720-24-C-24
    Internal IP   : 127.1.0.38
    Management IP : 10.17.10.38
Node :2
    Serial Number : BZA0330G00P
```

```
    Condition     : Good
    Status        : Connected to Cluster
    VCS Id        : 1
    Rbridge-Id    : 80*
    Co-ordinator  : NO
    WWN           : 10:00:00:05:33:78:00:00
    Switch MAC    : 00:05:33:78:00:81
    FCF MAC       : 19:30:00:48:19:31
    Switch Type   : Brocade VDX 8770-4
    Internal IP   : 127.1.0.80
    Management IP : 10.17.11.80
Node :3
    Serial Number : BWW2516G01G
    Condition     : Good
    Status        : Connected to Cluster
    VCS Id        : 1
    Rbridge-Id    : 82
    Co-ordinator  : NO
    WWN           : 10:00:00:05:33:6F:2B:D2
    Switch MAC    : 00:05:33:6F:2B:D2
    FCF MAC       : 0B:20:B0:64:10:26
    Switch Type   : Elara2f
    Internal IP   : 127.1.0.82
    Management IP : 10.17.10.82
(output truncated)
```

To issue the **show vcs** command on a VCS-disabled switch:

```
switch# show vcs
state      : Disabled
```

To display the virtual IP address:

```
switch# show vcs virtual-ip
Virtual IP                : 10.21.87.2/20
Associated rbridge-id     : 2
```

See Also **vcs**

show version

Displays the current firmware version.

Synopsis **show version** [**rbridge-id** {*rbridge-id* | **all** }*]* [**all-partitions**][**brief**]

Operands

rbridge-id	Executes the command on the specified switch.
rbridge-id	Specifies the unique identifier for the switch.
brief	Displays a brief version of the firmware information.
all-partitions	Displays firmware information for both the active and the standby partitions. For each module, both partitions are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display firmware version information and build dates. The default command output includes the following information:

Network Operating System Version	The firmware version number
Firmware name	The label of the firmware image
Build Time	The build date and time of the firmware
Install time	The date and time of the firmware installation
Kernel	The Linux kernel version
Boot-Prom	The size of the boot programmable read-only memory.
Control Processor	The control processor model and memory

Usage Guidelines When executed on the active management module, this command displays firmware versions on both management modules and interface modules. When executed on the standby management module, only the firmware versions for the standby management module are displayed.

The **rbridge-id** and **all** operands are not supported.

Examples To display the firmware version information for all partitions:

```
switch# show version all-partitions
Network Operating System Software
Network Operating System Version: 3.0.0
Copyright (c) 1995-2012 Brocade Communications Systems, Inc.
Firmware name:      3.0.0
Build Time:         01:18:17 May 26, 2012
Install Time:       10:16:24 May 27, 2012
Kernel:             2.6.34.6
BootProm:           1.0.0
Control Processor:  e500mc with 7168 MB of memory

Slot    Name    Primary/Secondary Versions    Status
-----------------------------------------------------
 M1     NOS     3.0.0                         STANDBY
                3.0.0
```

```
 M2     NOS     3.0.0                                    ACTIVE*
                3.0.0
 L1/0   NOS     3.0.0                                    ACTIVE
                3.0.0
 L1/1   NOS     3.0.0                                    STANDBY
                3.0.0
 L2/0   NOS     3.0.0                                    ACTIVE
                3.0.0
 L2/1   NOS     3.0.0                                    STANDBY
                3.0.0
```

To display the firmware for all partitions in the brief view:

```
switch# show version all-partitions brief

Slot    Name    Primary/Secondary Versions               Status
-----------------------------------------------------------------
 M1     NOS     3.0.0                                    STANDBY
                3.0.0
 M2     NOS     3.0.0                                    ACTIVE*
                3.0.0
 L1/0   NOS     3.0.0                                    ACTIVE
                3.0.0
 L1/1   NOS     3.0.0                                    STANDBY
                3.0.0
 L2/0   NOS     3.0.0                                    ACTIVE
                3.0.0
 L2/1   NOS     3.0.0                                    STANDBY
                3.0.0
```

See Also firmware download, show firmwaredownloadstatus

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. Refer to "Usage Guidelines" below.
brief	Specifies to display VLAN information for all interfaces including static and dynamic.
classifier	Specifies to display all VLAN classification information.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about VLAN.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To show information on a VLAN:

```
switch# show vlan 1
VLAN     Name            State   Ports

                                 (u)-Untagged, (t)-Tagged

                                 (c)-Converged
======= ================ ======= ==============================
1       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* | **interface port-channel** *number* | **rule** *number* | **interface tengigabitethernet** *rbridge-id/slot/port* | **interface gigabitethernet** *rbridge-id/slot/port*]

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.

interface 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.

interface tengigabitethernet
Specifies a valid 10 Gbps Ethernet interface.

rbridge-id Specifies a switch by its RBridge identifier.

slot Specifies a valid slot number.

port Specifies a valid port number.

interface gigabitethernet
Specifies a valid 1 Gbps Ethernet interface.

rbridge-id Specifies a switch by its RBridge identifier.

slot Specifies a valid slot number.

port Specifies a valid port number

Defaults None

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.

The **interface gigabitethernet** *rbridge-id/slot/port* operand is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8.

Examples None

See Also None

show vnetwork

Displays virtual assets from the vCenter that are discovered on the Brocade VDX switch.

Synopsis **show vnetwork [dvs {all | *name*} | dvpgs {all | *name*} | pgs {all | *name*} | hosts {all | *name*} | vcenter status | vmpolicy {all | macaddr *address*} | vms {all | *name*} | vss {all | *name*}]**

Operands

dvs	Displays discovered distributed virtual switches.
all	Displays all associated information.
name	Text string for the name. If the name includes spaces, enclose the string in quotes.
dvpgs	Displays discovered distributed virtual port groups.
all	Displays all associated information.
name	Text string for the name. If the name includes spaces, enclose the string in quotes.
pgs	Displays discovered standard port groups.
all	Displays all associated information.
name	Text string for the name. If the name includes spaces, enclose the string in quotes.
hosts	Displays discovered hosts.
all	Displays all associated information.
name	Text string for the name. If the name includes spaces, enclose the string in quotes.
vcenter status	Displays configured vCenter status.
vmpolicy	Displays the following network policies on the Brocade VDX switch: associated media access control (MAC) address, virtual machine, (dv) port group, and the associated port profile.
all	Displays all associated information.
macaddr *address*	The six octet MAC address; for example, 00:50:56:8e:00:4b.
vms	Displays discovered VMs.
all	Displays all associated information.
name	Text string for the name. If the name includes spaces, enclose the string in quotes.
vss	Displays discovered standard virtual switches.
all	Displays all associated information.
name	Text string for the name. If the name includes spaces, enclose the string in quotes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view the following virtual assets that are configured on the vCenter and discovered on the VDX switch.

Usage Guidelines None

Examples

```
switch# show vnetwork ?
Possible completions:
  dvpgs      Shows discovered distributed virtual port-groups
  dvs        Shows discovered distributed virtual switches
  hosts      Shows discovered hosts
  pgs        Shows discovered standard port-groups
  vcenter    Shows configured vCenter
  vmpolicy   Shows vnics/vmknics to portgroup to port-profile association
  vms        Shows discovered VMs
  vss        Shows discovered standard virtual switches
```

```
switch# show vnetwork dvpgs
dvPortGroup                          dvSwitch                          Vlan
==================================== ================================= =========
ProductionVMs                        dvSwitch-Production               10-10,
dvSwitch-Production-DVUplinks-7589   dvSwitch-Production               0-4094,
```

```
switch# show vnetwork dvs
dvSwitch                      Host        Uplink Name    Switch Interface
========                      =========== ============== ================
dvSwitch-Production40         -           -              -
dvSwitch-Production41         -           -              -
Total Number of Entries: 2
```

NOTE
The switch interface column information is local to each switch in the fabric.

```
switch# show vnetwork hosts
Host                          Uplink Name  Uplink MAC       (d)Virtual Switch      Switch Interface
====                          ===========  =========         ================      ===============
ESX-4921.englab.brocade.com   vmnic0       e4:1f:13:43:54:90 vSwitch0               -
                              vmnic2       00:1b:21:8f:4a:f0 dvSwitch-Production    115/0/5
                              vmnic4       00:05:33:26:3e:ba vSwitch1               115/0/1
                              vmnic5       00:05:33:26:3e:bb dvSwitch-Production    -
ESX-4922.englab.brocade.com   vmnic0       e4:1f:13:43:95:5c vSwitch0               -
                              vmnic2       00:05:33:26:2d:90 dvSwitch-Production    115/0/10
                              vmnic3       00:05:33:26:2d:91 dvSwitch-Production    115/0/11
                              vmnic5       00:05:1e:eb:f9:94 vSwitch1               115/0/2
```

NOTE
The switch interface column information is local to each switch in the fabric.

```
switch# show vnetwork pgs
PortGroup    vSwitch         vlanId        Host
============ =============== ============= ============================
TestVMs      vSwitch1        50-50,        ESX-4922.englab.brocade.com
             vSwitch1        50-50,        ESX-4921.englab.brocade.com
VMkernel     vSwitch1        0-0,          ESX-4922.englab.brocade.com
```

```
            vSwitch1        0-0,          ESX-4921.englab.brocade.com

switch# show vnetwork vcenter status
vCenter          Start                Elapsed (sec)  Status
================ ==================== ============== ================
MYVC             2011-09-07 14:08:42  10             In progress


switch# show vnetwork vmpolicy macaddr all
Associated MAC    Virtual Machine             (dv)PortGroup      Port-Profile
================= =========================== ================== ==================
00:50:56:72:42:4c -                           ProductionVMs      auto-ProductionVMs
00:50:56:78:69:36 -                           VMkernel           auto-VMkernel
00:50:56:7b:e5:41 -                           ProductionVMs      auto-ProductionVMs
00:50:56:7d:96:16 -                           VMkernel           auto-VMkernel
00:50:56:8e:00:4b CentOS-4921                 ProductionVMs      auto-ProductionVMs
00:50:56:8e:00:4d CentOS-4921                 TestVMs            auto-TestVMs
00:50:56:8e:00:50 CentOS-4922                 TestVMs            auto-TestVMs
00:50:56:8e:00:51 CentOS-4922                 ProductionVMs      auto-ProductionVMs


switch# show vnetwork vms
Virtual Machine            Associated MAC    IP Addr     Host
========================== ================= =========== ==========================
CentOS-4921                00:50:56:8e:00:4b -           ESX-4921.englab.brocade.com
                           00:50:56:8e:00:4d -           ESX-4921.englab.brocade.com
CentOS-4922                00:50:56:8e:00:50 -           ESX-4922.englab.brocade.com
                           00:50:56:8e:00:51 -           ESX-4922.englab.brocade.com

vSwitch           Host                            Uplink Name    Switch Interface
================= =============================== ============== ================
vSwitch0          djesxi-5064.englab.brocade.com vmnic0         -
                                                  vmnic1         -
                  ht-153.englab.brocade.com       vmnic0         -
                  ht-154.eng.brocade.com          vmnic0         -
vSwitch1          ht-153.englab.brocade.com       vmnic7         -
                  ht-154.eng.brocade.com          vmnic6         -
                                                  vmnic7         -
vSwitch2          ht-153.englab.brocade.com       vmnic6         -
Total Number of Entries: 8
```

NOTE

The switch interface column information is local to each switch in the fabric.

See Also show port-profile, vcenter

show vrrp

Displays information about VRRP and VRRP-E sessions.

Synopsis

show vrrp *VRID* [**detail**] [**summary**]

show vrrp detail

show vrrp interface [**detail**] [**summary**]

show vrrp summary

Operands

VRID	The virtual-group ID about which to display information. Range is 1 to 128.
detail	Displays all session information in detail, including session statistics.
summary	Displays one-line, session-information summaries.
interface	Displays information for an interface that you specify.

FortyGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 40-Gbps port interface.

rbridge-id	Specifies the ID of the routing bridge. This operand is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

GigabitEthernet *rbridge-id/slot/port*
Specifies a valid 1-Gbps Ethernet interface

rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

TenGigabitEthernet *rbridge-id/slot/port*
Specifies a valid 10-Gbps Ethernet interface.

rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.

Default None.

Command Modes Privileged EXEC mode.

Description Displays information about VRRP and VRRP-E sessions, either in summary or full-detail format. Can also specify a particular virtual group or interface for which to display output.

Usage Guidelines This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** interface type. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples To show all session information in detail, including session statistics:

```
switch# show vrrp detail
VRID 1
  Interface: TengigabitEthernet 0/18;  Ifindex: 403832850
  Mode: VRRP
  Admin Status: Enabled
  Address family: IPv4
  Authentication type: No Authentication
  State: Master
  Virtual IP(s): 1.1.1.5, 1.1.1.6, 1.1.1.8, 1.1.1.9

  Configured Priority: 255  (default: 100); Current Priority: 255
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority
    =======                   ========
  Statistics:
    Advertisements: Rx: 0, Tx: 10298
    ARP:            Rx: 0, Tx: 28

VRID 2
  Interface: TengigabitEthernet 0/22;  Ifindex: 404094998
  Mode: VRRP
  Admin Status: Disabled
  Address family: IPv4
  Authentication type: No Authentication
  State: Initialize
  Virtual IP: unset
  Configured Priority: 100  (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority
    =======                   ========
  Statistics:
    Advertisements: Rx: 0, Tx: 0
    ARP:            Rx: 0, Tx: 0

VRID 3
  Interface: TengigabitEthernet 0/18;  Ifindex: 403832850
  Mode: VRRP
  Admin Status: Enabled
  Address family: IPv4
  Authentication type: No Authentication
  State: Master
  Virtual IP(s): 1.1.1.20
  Configured Priority: 100  (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority
    =======                   ========
  Statistics:
    Advertisements: Rx: 0, Tx: 9785
    ARP:            Rx: 0, Tx: 2
```

show zoning operation-info

Displays information about transactions and database size.

Synopsis **show zoning operation-info**

Operands None

Defaults None

Command Modes Privileged EXEC mode.

Description Use this command to display the size details of the zone database and transaction token information for a Brocade VCS Fabric.

db-max Defines the maximum size in bytes of the zone database in nonvolatile memory.

db-avail Displays the size in bytes of the unused portion of nonvolatile memory available for the defined configuration.

db-committed Displays the size in bytes of the defined configuration currently stored in nonvolatile memory.

db-transaction Displays the size in bytes of the uncommitted defined configuration.

db-token Displays the current transaction token ID.

last-zone-changed-timestamp Displays the last time the defined zone configuration was modified.

last-zone-committed-timestamp Displays the data and time of the last time the zoning database was saved to nonvolatile memory.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge.

Examples To display information about transactions and database size:

```
switch# show zoning operation-info
db-max 1045274
db-avail 1043822
db-committed 440
db-transaction 0
transaction-token 0
last-zone-changed-timestamp 2011-11-16 14:38:15 GMT-7:00
last-zone-committed-timestamp 2011-11-16 14:38:15 GMT-7:00
```

See Also show running-config zoning defined-configuration, show running-config zoning enabled-configuration

shutdown

Disables the selected interface.

Synopsis **shutdown**

no shutdown

Operands None

Defaults The interface is disabled.

Command Modes Interface subconfiguration mode (Fcoe, fibre channel, fo, gi, loopback, port-channel, te, Ve, VLAN).

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 a specific tengigabit ethernet interface:

```
switch(config)# interface tengigabitethernet 1/0/1
switch(conf-if-te-1/0/1)# shutdown
```

To enable a specific gigabitethernet interface:

```
switch(config)# gigabitethernet interface 1/0/2
switch(conf-if-gi-1/0/2)# no shutdown
```

See Also interface, interface Ve, 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.

Usage Guidelines 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
switch(conf-rstp)# shutdown
```

To enable STP globally:

```
switch(config)# protocol spanning-tree rstp
switch(conf-rstp)# no shutdown
```

See Also None

shutdown-time

Specifies the time a port will be disabled after Edge Loop Detection (ELD) detects a loop.

Synopsis **shutdown-time** *period*

no shutdown-time *period*

Operands

period	Specifies the number of minutes before re-enabling a port. The range of values is 10 through 1440 (10 minutes through 24 hours).

Defaults The default value is zero (0). The port will not be re-enabled automatically.

Command Modes ELD configuration mode.

Description Use this command to specify the time between ELD shutting down a port because it has detected a loop and re-enabling that port automatically. Use the **no shutdown-time** command to return to the default value.

Any change to **shutdown-time** only takes effect for the ports that are disabled by ELD after the configuration change. Any ports that were already disabled by ELD before the **shutdown-time** change continues to follow the old **shutdown-time** value. These ports start to follow the new shutdown time after the currently running timer expires and ELD still detects the loop and shuts down the port again.

Usage Guidelines If you do not set a shutdown time using this command, you can re-enable all ELD-disabled ports manually using the **clear edge-loop-detection** command.

Examples To re-enable ports 24 hours after they are disabled by ELD:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# shutdown-time 1440
```

To cancel automatic port re-enable:

```
switch(config-eld)# no shutdown-time 1440
```

See Also clear edge-loop-detection, show edge-loop-detection globals, show edge-loop-detection rbridge-id

snmp-server

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* | *ipv6_host* | *dns_host*} [**version** {**1** | **2c**}] [**udp-port** *port*] [**severity-level** {**none** | **debug** | **info** | **warning** | **error** | **critical**}]

no snmp-server host *ipv4_host* | *ipv6_host* | **dns_host** [**version** {**1** | **2c**}] [**udp-port** *port*] [**severity-level** {**none** | **debug** | **info** | **warning** | **error** | **critical**}]

Operands

host {*ipv4_host* | *ipv6_host* | *dns_host*}
Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

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 from 0 through 65535.

severity-level {**none** | **debug** | **info** | **warning** | **error** | **critical**}]
Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASlog (swEvent) traps can be filtered based on severity level. If the severity level of None is specified, all traps are filtered and no RASlog traps are received. If the severity level of Critical is specified, no traps are filtered and all traps are received by the host.

Defaults

- The default UDP port is 162.
- The default SNMP version is 1.
- The default severity level is None.

Command Modes Global configuration mode

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.

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 host 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 from 2 through 16 characters. The values for the community strings are:

The following community strings are read-write:

- Secret Code
- OrigEquipMfr
- private

The following community strings are read-only:

- public
- common
- ConvergedNetwork

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 must be deleted.

The **no snmp-server host** *host* **community-string** *string* **version** *2c* command brings version 2c down to version 1.

The **no snmp-server host** *host* **community-string** *string* command removes the SNMP server host from the switch configuration altogether.

Examples The following **snmp-server host** *ipv6_host* command creates an entry for trap host 1050:0:0:0:5:600:300c:326b associated with community "public." The trap host receives traps from the configured switch.

```
switch(config)# snmp-server host 1050:0:0:0:5:600:300c:326b public severity-level
Info
```

The following **snmp-server host** *dns_host* command creates an entry for trap host brcd.brocade.com associated with community "public." The trap host receives traps from the configured switch.

```
switch(config)# snmp-server host brcd1.brocade.com public severity-level Info
```

The following **snmp-server host** *ipv6_host* command creates an entry for SNMPv3 trap IPv6 host 1050:0:0:0:5:600:300c:326b associated with SNMP user "snmpadmin2." The trap host will receive SNMPv3 traps from the configured switch.

```
switch(config)# snmp-server v3host 1050::5:600:300c:326b snmpadmin2
severity-level Info
```

The following **snmp-server host** *dns_host* command creates an entry for SNMPv3 trap host brocade.com associated with SNMP user "snmpadmin3." The trap host will receive SNMP V3 traps from the configured switch.

```
switch(config)# snmp-server v3host brocade.com snmpadmin3 severity-level Info
```

The following **snmp-server host** *dns_host_for_inform* command creates an entry for SNMPv3 informs host "brocade.com" associated with SNMP user "snmpuser 3."

```
switch(config)# snmp-server v3host brocade.com snmpuser3 notifytype informs
engineid 80:00:05:23:01:AC:1A:01:F6 severity-leInfo
```

To associate "commaccess" as a read-only community and set 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
```

To create a trap host (10.23.23.45) associated with the community "public", which will receive all traps with the severity levels of Info, Warning, Error, and Critical:

```
switch(config)# snmp-server host 10.23.23.45 public severity-level info
```

To reset the severity level to None:

```
switch(config)# snmp-server host 10.23.23.45 public severity-level none
```

See Also show running-config snmp-server, snmp-server community, snmp-server contact, snmp-server location, snmp-server user, snmp-server v3host

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.

Defaults If no access is specified, read-only (ro) is the default.

Command Modes Global configuration mode

Description Use this command to manage the configuration of the SNMP agent in the switch. The configuration includes SNMPv1 and SNMPv2c configuration settings.

Usage Guidelines 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.

The following community strings are read-write:

- Secret Code
- OrigEquipMfr
- private

The following community strings are read-only:

- public
- common
- ConvergedNetwork

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, snmp-server contact, snmp-server, snmp-server location, snmp-server user, snmp-server v3host**

snmp-server contact

Sets the SNMP server contact string.

Synopsis **snmp-server contact** *string*

no snmp-server contact *string*

Operands

string	Specifies the server contact. You must enclose the text in double quotes if the text contains spaces.

Defaults The default contact string is “Field Support”.

Command Modes Global configuration mode

Description Use this command to set the SNMP server contact string.

Usage Guidelines Use the **no snmp-server contact** *string* command to restore the default values.

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, snmp-server community, snmp-server, snmp-server location, snmp-server user, snmp-server v3host**

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. You must enclose the text in double quotes if the text contains spaces.

Defaults By default, the location is set to “End User Premise.”

Command Modes Global configuration mode

Description Use this command to set the SNMP server location string.

Usage Guidelines None

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, snmp-server community, snmp-server contact, snmp-server, snmp-server user, snmp-server v3host**

snmp-server sys-descr

Sets the Management Information Base (MIB-2) object identifier (OID) system description.

Synopsis **snmp-server sys-descr** *string*

no snmp-server sys-descr

Operands

string	The text for the system description. The range of valid characters is from 4 through 255 characters.

Defaults The default system description is “Brocade VDX switch”.

Command Modes Global configuration mode

Description Use the **snmp-server sys-descr** command to specify the MIB-2 OID description.

Usage Guidelines None

Examples To set the system description OID to “Brocade Cluster switch”:

```
switch(config)# snmp-server sys-descr “Brocade Cluster switch”
```

To set the system description OID to the default, “Brocade VDX switch”:

```
switch(config)# no snmp-server sys-descr
```

See Also **show running-config snmp-server, snmp-server community, snmp-server contact, snmp-server, snmp-server location, snmp-server user**

snmp-server user

Creates or changes the attributes of users that are associated with SNMP version 3.

Synopsis **snmp-server user** *username* [**groupname** *group-name*] [**auth**] {**md5** | **sha**} [**auth-password** *string*] [**priv**] {**DES** | **AES128**} [**priv-password** *string*]

no snmp-server user *user-name*

Operands

username	The name of the user that connects to the agent. The length of the user name must be from 1 through 16 characters in length.
groupname *group-name*	The name of the group to which the user is associated: snmpadmin is a read-write group and snmpuser is a read-only group.
auth	Initiates an authentication level setting session.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
auth-password *string*	A string that enables the agent to receive packets from the host. Passwords are plain text and must be added each time for each configuration replay. The password must be from 1 through 32 characters in length.
priv	Initiates a privacy authentication level setting session. By default, this option is disabled.
DES	Specifies the DES privacy protocol.
AES128	Specifies the AES128 privacy protocol.
priv-password *string*	A string (not to exceed 32 characters) that enables the host to encrypt the contents of the message that it sends to the agent. Passwords are plain text and must be added each time for each configuration replay.

Defaults By default, two groups are configured; snmpadmin and snmpuser.

By default, the **auth** operand is turned off.

By default, the **priv** operand is turned off.

By default, six users are added. The three read-write users are "snmpadmin1", "snmpadmin2", and "snmpadmin3". The three read-only users are "snmpuser1", "snmpuser2", and "snmpuser3".

Command Modes Global configuration mode

Description The **snmp-server user** command configures SNMPv3 users that can be associated to a trap and inform response functionality. To add a new user to either group, one of the default users must be deleted.

Usage Guidelines Use the **no snmp-server user** *user-name* command to delete a user.

Examples To configure an authentication policy:

```
switch(config)# snmp-server user brocade groupname snmpadmin auth md5 user123
priv des user456
```

See Also show running-config snmp-server, snmp-server community, snmp-server contact, snmp-server, snmp-server location, snmp-server v3host

snmp-server v3host

Specifies the recipient of the SNMP version 3 notification option.

Synopsis **snmp-server v3host** [**host** {**ipv4_host** | **ipv6_host** | **dns_host**}] [**notifytype** {**traps**|**informs**}] **engineid** *engine-id* **udp-port** *port_number* [**severity-level** {**none** | **debug** | **info** | **warning** | **error** | **critical**}]

no snmp-server v3host [**host** {**ipv4_host** | **ipv6_host** | **dns_host**}]

Operands **host** {**ipv4_host** | **ipv6_host** | **dns_host**}

Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

notifytype {**traps** | **informs**}

Specifies the type of notification traps that are sent for the host. Traps and informs are supported.

engineID *engine-id* Configures the remote engine ID to receive informs on a remote host.

udp-port *port_number* Specifies the UDP port of the host.

severity-level {**none** | **debug** | **info** | **warning** | **error** | **critical**}]
Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASlog (swEvent) traps can be filtered based on severity level. If the severity level of None is specified, all traps are filtered and no RASlog traps are received. If the severity level of Critical is specified, no traps are filtered and all traps are received by the host.

Defaults None

Command Modes Global configuration mode

Description Use the **snmp-server v3host** command to specify the recipient of SNMP version 3 notifications.

Usage Guidelines Use the **no snmp-server v3host** [**host** {**ipv4_host** | **ipv6_host** | **dns_host**}] command to remove a host.

Examples None

See Also **show running-config snmp-server, snmp-server community, snmp-server contact, snmp-server, snmp-server location, snmp-server user**

source

Configures the monitoring session.

Synopsis **source** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **destination** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **direction [rx | tx | both]**

no source [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **destination** [**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **direction [rx | tx | both]**

Operands

tengigabitethernet	Specifies a valid external 10 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
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.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
gigabitethernet	Specifies a valid 1 Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge. This is not valid in standalone mode.
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 None

Command Modes Monitor session configuration mode

Description Use this command to enable a session for monitoring traffic. Use the **no** version of this command to delete the port mirroring connection.

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 22 for monitoring traffic:

```
switch(config)# monitor session 22
switch(config-session-22)# source tengigabitethernet 0/1 destination
tengigabitethernet 0/15 direction both
```

See Also monitor session

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 subconfiguration mode (fo, gi, port-channel, te).

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.

This command does not function in VCS mode.

Examples To enable automatic edge detection:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree autoedgeb
```

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 None

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

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 R-PVST+.

This command does not function in VCS mode.

Brocade Network OS v3.0.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Usage Guidelines Use the **no spanning-tree bpdu-mac 0100.0ccc.cccd** command to remove the address.

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 200000000.
vlan *vlan_id*	Specifies the VLAN ID. Refer to "Description" below.

Defaults The default path cost is 200000000.

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to configure the path cost for spanning-tree calculations.

If the VLAN parameter is not provided, the cost is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Usage Guidelines Lower path cost indicates a greater chance of becoming root.

This command does not function in VCS mode.

Examples To set the port cost to 128:

```
switch(config)# interface tengigabitethernet 0/1
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 subconfiguration mode (fo, gi, port-channel, te).

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 This command does not function in VCS mode.

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 enable a port to quickly transition to the forwarding state:

```
switch(config)# interface tengigabitethernet 0/1
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(config)# interface tengigabitethernet 0/1
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** *vlan_id*]

no spanning-tree guard root

Operands **vlan** *vlan_id* Specifies the VLAN ID. Refer to "Description" below.

Defaults Guard root is disabled.

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

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.

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.

If the VLAN parameter is not provided, the guard root functionality is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Usage Guidelines The root port provides the best path from the switch to the root switch.

This command does not function in VCS mode.

Examples To enable guard root:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree guard root
```

See Also **show spanning-tree**

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 subconfiguration mode (fo, gi, port-channel, te).

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.

This command does not function in VCS mode.

Examples To set the hello time to 5 seconds:

```
switch(config)# interface tengigabitethernet 0/1
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 32.
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 subconfiguration mode (fo, gi, port-channel, te).

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.

This command does not function in VCS mode.

Examples To set restrictions for the port of MSTP instance 1 with the cost of 40000:

```
switch(config)# interface tengigabitethernet 0/1
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 subconfiguration mode (fo, gi, port-channel, te).

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.

This command does not function in VCS mode.

Examples To specify the link type as shared:

```
switch(config)# interface tengigabitethernet 0/1
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 subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to enable the Port Fast feature. This command 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.

Enable Port Fast on ports connected to host. Enabling Port Fast on interfaces connected to switches, bridges, hubs, and so on can cause temporary bridging loops, in both trunking and non-trunking mode.

This command does not function in VCS mode.

Examples To enable a port to quickly transition to the forwarding state:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree portfast
```

To set the Port Fast BPDU filter for the port:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree portfast bpdu-filter
```

To guard the port against the reception of BPDUs:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree portfast bpdu-guard
```

See Also **show spanning-tree**, 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 ID. Refer to "Description" below.

Defaults The default value is 128.

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

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.

If the VLAN parameter is not provided, the priority is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Usage Guidelines This command does not function in VCS mode.

Examples To configure the port priority to 16:

```
switch(config)# interface tengigabitethernet 0/1
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 subconfiguration mode (fo, gi, port-channel, te).

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.

This command does not function in VCS mode.

Usage Guidelines None

Examples To configure the port from becoming a root port:

```
switch(config)# interface tengigabitethernet 0/1
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 subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to restrict the topology change notification Bridge Protocol Data Units (BPDUs) sent on the port.

This command does not function in VCS mode.

Usage Guidelines Use the **no spanning-tree restricted-tcn** command to disable this option.

Examples To restrict the TCN on a specific interface:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# 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 subconfiguration mode (fo, gi, port-channel, te).

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.

This command does not function in VCS mode.

Usage Guidelines None

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

speed (Ethernet)

Sets the speed on the Ethernet interface.

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

no speed

Operands

10000	Forces the speed to 10 Gbps.
1000	Forces the speed to 1 Gbps.
auto	Allows the interface to negotiate the speed setting.

Defaults The default setting for this command is **auto**.

Command Modes Tengigabitethernet interface subconfiguration mode.

Description Use this command to set the speed negotiation value for a specific interface.

Usage Guidelines The speed command is not available for gigabitethernet or fortygigabitethernet ports.

Use the **no speed** command to return to the default.

Examples To set the speed to 10 Gbps on a specific Tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 170/0/1
switch(conf-if-int-170/0/1)# speed 10000
```

See Also interface

speed (Fibre Channel)

Sets the operational speed of a Fibre Channel port.

Synopsis **speed** {**auto** | **1gbps** | **2gbps** | **4gbps** | **8gbps**}

Operands

auto	Allows the interface to negotiate the port speed.
1gbps	Sets the operational port speed to 1 Gbps.
2gbps	Sets the operational port speed to 2 Gbps.
4gbps	Sets the operational port speed to 4 Gbps.
8gbps	Sets the operational port speed to 8 Gbps.

Defaults The default value is **auto**.

Command Modes Fibre channel interface subconfiguration mode.

Description Use this command to set the operational speed for a Fibre Channel port.

Usage Guidelines The Fibre Channel version of this command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples To set the Fibre Channel port speed:

```
switch (config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# speed 4gbps
```

See Also **desire-distance**, **fill-word**, **interface**, **isl-r_rdy**, **long-distance**, **show running-config interface FibreChannel**, **shutdown**, **trunk-enable**, **vc-link-init**

speed (Port-channel)

Sets the speed on the port-channel interface.

Synopsis **speed** {**1000** | **10000** | **40000**}

no speed

Operands

1000	Forces the speed to 1 Gbps.
10000	Forces the speed to 10 Gbps.
40000	Forces the speed to 40 Gbps.

Defaults The default setting for this command is 10000.

Command Modes Port-channel interface subconfiguration mode.

Description Use this command to set the speed negotiation value for a specific port-channel interface.

Usage Guidelines Use the **no speed** command to return to the default.

Examples To set the speed to 40 Gbps on a specific port-channel interface:

```
switch(config)# interface port-channel 44
switch(config-Port-Channel-44)# speed 40000
```

See Also **interface**

speed (LAG)

Sets the speed on the LAG interface.

Synopsis **speed** {**1000** | **10000** | **40000**}

Operands

1000	Forces the speed to 1 Gbps.
10000	Forces the speed to 10 Gbps.
40000	Forces the speed to 40 Gbps.

Defaults The default setting for this command is 10000

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.

Examples None

See Also None

ssh

Connects to a remote server using the Secure Shell (SSH) protocol.

Synopsis **ssh** [**-c**] [**-l**] [**-m**] {*IP Address* | *hostname*}

Operands

-c		Specifies the encryption algorithm for the SSH session. This operand is optional; if no encryption algorithm is specified, the default (**3des**) is used. Supported algorithms include the following:
	3des	Triple Data Encryption Standard (DES). This is the default setting.
	aes128-cbc	AES 128-bits
	aes192-cbc	AES 192-bits
	aes256-cbc	AES 256-bits
-l *username*		Login name for the remote server. This operand is optional. If you specify a username, you will be prompted for a password. If you don't specify a username, the command assumes you are logging in as root and will prompt for the root password.
-m		Specifies the HMAC (Hash-based Message Authentication Code) message encryption algorithm. This operand is optional; if no encryption algorithm is specified, the default (**hmac-md5)** is used. Supported algorithms include the following:
	hmac-md5	MD5 128-bits. This is the default setting.
	hmac-md5-96	MD5 96-bits
	hmac-sha1	SHA1 160-bits
	hmac-sha1-96	SHA1 96-bits
IP Address		Specify the server IP address in IPv4 or IPv6 format.
hostname		Alternately, specify the host name, a string between 1 and 253 characters long.

Defaults SSH connects to port 22. Refer to the operand descriptions for operand-specific defaults.

Command Modes Privileged EXEC mode

Description Use this command to establish an encrypted SSH connection from a switch to a remote networking device. This implementation is based on SSH v2.

Usage Guidelines The following features are not supported:

- Displaying SSH sessions
- Deleting stale SSH keys

Examples To connect to a remote device using an SSH connection with default settings:

```
switch# ssh 10.70.212.152

The authenticity of host '10.70.212.152 (10.70.212.152)' can't be
established.
```

```
RSA key fingerprint is f0:2a:7e:48:60:cd:06:3d:f4:44:30:2a:ce:68:fe:1d.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.70.212.152' (RSA) to the list of known hosts.
Password:
```

To connect to a remote device using an SSH connection with a login name:

```
switch# ssh -l admin 127.2.1.8
admin@127.2.1.8's password
```

See Also show running-config ssh server, show ssh server status, ssh server shutdown, telnet

ssh server shutdown

Disables ssh service on the switch.

Synopsis **ssh server shutdown**

no ssh server shutdown

Operands None

Defaults None

Command Modes Global configuration mode

Description This command disables ssh service on the switch.

Usage Guidelines Use the **no ssh server shutdown** command to enable ssh service.

Examples None

See Also **show running-config ssh server**, **show ssh server status**

storm-control ingress

Limits ingress traffic on a specified interface.

Synopsis **storm-control ingress** {**broadcast** | **unknown-unicast** | **multicast**} {**limit-bps** | **limit-percent** } *rate* [{**monitor** | **shutdown**] }

no storm-control ingress {**broadcast** | **unknown-unicast** | **multicast**} {**limit-bps** | **limit-percent** } *rate* [{**monitor** | **shutdown**] }

Operands

broadcast	Specifies that the command will operate on broadcast traffic only.
unknown-unicast	Specifies that the command will operate on unknown-unicast traffic only.
multicast	Specifies that the command will operate on multicast traffic only.
limit-bps	Specifies that the value given to the *rate* operand is in bits per second. If the traffic on the interface reaches this rate, no more traffic (for the traffic type specified) is allowed on the interface.
limit-percent	Specifies that the value given to the *rate* operand is in percentage of capacity of the interace. If the traffic on the interface reaches this percentage of capacity, no more traffic (for the traffic type specified) is allowed on the interface.
rate	Specifies the amount of traffic allowed, either in bits per second or a percentage of the capacity of the interface, depending on which operand was chosen with the rate. • Range if you are specifying rate in bps: 0 to 10000000000. Because each application-specific integrated circuit (ASIC) may support different bit granularity, bit rates are rounded up to the next achievable rate. • Range if you are specifying rate in percent of interface capacity: 0 to 100.
monitor	Specifies that, if a rate limit is reached within a five-second sampling period, a log message gets sent. A log message is generated upon the first occurrence of such an event. Subsequent log messages are generated only at the end of one complete sample interval in which no rate limits are reached.
shutdown	Specifies that, if a rate limit is exceeded within a five-second sampling period, the interface will be shut down. You must manually re-enable the interface after a shutdown.

Default None

Command Modes Interface subconfiguration mode (fo, gi, te).

Description BUM storm control allows you to limit the amount of broadcast, unknown unicast, and multicast ingress traffic on a specified interface. The *shutdown* option monitors the status of the configured rate limit every five seconds, and if the maximum defined rate is exceeded the corresponding interface is shut down until you re-enable it using the **no shut** command.

Usage Guidelines This command is supported on the 8770-4 and 8770-8 platforms only. Use the **no** form of the command to disable BUM storm control for a particular traffic type on an interface.

If you want to modify an active BUM storm control configuration, you must first disable it, then issue the **storm-control ingress** command again with the new parameters.

Examples To configure storm control on a tengigabitethernet interface 101/0/2, with a limit-rate of 1000000 bps:

```
Switch (config)# interface tengigabitethernet 101/0/2
Switch (conf-if-te-101/0/2)# storm-control ingress broadcast 1000000
```

To disable BUM storm control for broadcast traffic only, on a tengigabitethernet interface 101/0/2:

```
Switch (config)# int te  101/0/2
Switch (conf-if-te-101/0/2)# no storm-control ingress broadcast
```

See Also interface, storm-control ingress, show storm-control, clear counters storm-control

summary-address

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Synopsis **summary-address** *A.B.C.D E.F.G.H*

Operands

A.B.C.D E.F.G.H	IP address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Default Summary addresses are not configured by default.

Command Modes Router configuration mode.

Description You can configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

You can configure up to 32 address ranges. The device sets the forwarding address of the aggregate route to zero and sets the tag to zero. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.

Usage Guidelines This option affects only imported, type 5 external routes. Use the **no** parameter to disable route summarization.

Examples To configure a summary address of 10.1.0.0 with a mask of 255.255.0.0:

```
switch(conf-ospf-router)# summary-address 10.1.0.0 255.255.0.0
```

The command in this example configures summary address 10.1.0.0, which includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. For all of these networks, only the address 10.1.0.0 is advertised in external LSAs.

support

Enables or disables the first-fault data capture (FFDC).

Synopsis **support [rbridge-id** *rbridge-id]* **ffdc**

no support [rbridge-id *rbridge-id]* **ffdc**

Operands

rbridge-id *rbridge-id*	Executes the command on a switch specified by its Rbridge ID. Only the local RBrige ID is supported.
ffdc	Enables FFDC.

Defaults FFDC is enabled by default.

Command Modes Global configuration mode

Rbridge ID 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 This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples To enable FFDC:

```
switch(config)# support rbridge-id 1
switch(config-rbridge-id-1)# ffdc
```

To disable FFDC:

```
switch(config)# support rbridge-id 1
switch(config-rbridge-id-1)# no ffdc
```

See Also **clear support, copy support,** show support

switch-attributes

Sets switch attributes.

Synopsis **switch-attributes** *rbridge-id*

chassis-name *string*

host-name *string*

no switch-attributes

Operands

rbridge-id Specifies the Rbridge ID for which to set the attribute. Only the local RBridge ID is supported.

chassis-name *string*
Sets the switch chassis name.

host-name *string*
Sets the switch host name.

Defaults The default chassis name depends on the switch model and can be one of the following product names:

- VDX 6720-24
- VDX 6720-60
- VDX 6730-32
- VDX 6730-76
- VDX 6710-54
- VDX 8770-4
- VDX 8770-8

The default host name is “sw0”.

Command Modes Global configuration mode

Description Use this command to set the switch attributes. When issued with the RBridge ID of the switch to be configured, this command goes into a sub-command shell where you can configure the host name or chassis name.

Usage Guidelines The text string for the **chassis-name** and **host-name** string is limited to 30 characters. The string must begin with a letter, and can consist of letters, digits, hyphens, and underscore characters. Spaces are not permitted.

Use the **no switch-attributes** command to restore the default values.

This command is not supported on the standby management module.

This command is supported only on the local switch.

Examples To set the host name for a switch with an rbridge ID of 2:

```
switch(config)# switch-attributes 2
switch(config-switch-attributes-1)# host-name VDX7620-24
switch(config-switch-attributes-1)# exit
```

See Also **show running-config switch-attributes**

switchport

Puts the interface in Layer 2 mode.

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 subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to put the interface in Layer 2 mode and to set the switching characteristics of the Layer 2 interface.

Usage Guidelines For changing the interface configuration mode to trunk or changing the default VLAN mapping, use additional **switchport** commands.

Use the **no switchport** command to take the switch out of the Layer 2 mode.

Examples To put a specific tengigabitethernet interface in Layer 2 mode:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport
```

To remove a specific port-channel interface from Layer 2 mode:

```
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no switchport
```

See Also **interface**, show vlan, **switchport mode**, switchport access, switchport trunk allowed vlan

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*. Refer to "Usage Guidelines" below.

Defaults By default, all Layer 2 interfaces are in access mode and belong to the VLAN ID 1.

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to set the Layer 2 interface as access. In access mode, the interface only allows untagged and priority tagged packets.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Use the **no switchport access vlan** command to set the PVID to the default VLAN 1.

Examples To set the Layer 2 interface PVID to 100 on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport access vlan 100
```

To set the PVID to the default VLAN 1 on a specific port-channel interface:

```
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no switchport access vlan
```

See Also **interface**, **show vlan**, **switchport mode**, **switchport trunk allowed vlan**, **switchport**

switchport mode

Sets the mode of the Layer 2 interface.

Synopsis **switchport mode {access | trunk}**

Operands

access	Sets the Layer 2 interface as access.
trunk	Sets the Layer 2 interface as trunk.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to set the mode of the Layer 2 interface. Access mode assigns the port to a VLAN. Trunk mode makes the port linkable to other switches and routers.

Usage Guidelines You must configure the same native VLAN on both ends of an 802.1q trunk link. Failure to do so can cause bridging loops and VLAN leaks.

Examples To set the mode of a specific tengigabitethernet interface to *access*:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode access
```

To set the mode of a specific port-channel interface to *trunk*:

```
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# switchport mode trunk
```

See Also **interface**, **show vlan**, **switchport access**, **switchport trunk allowed vlan**, **switchport**

switchport trunk allowed vlan

Adds or removes VLANs on a Layer 2 interface in trunk mode.

Synopsis **switchport trunk allowed vlan {add** *vlan_id* **| all | except** *vlan_id* **| none | remove** *vlan_id* **}**

Operands

add *vlan_id*	Adds a VLAN to transmit and receive through the Layer 2 interface. Refer to "Usage Guidelines" below.
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. Refer to "Usage Guidelines" below.
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. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to set the VLANs that will transmit and receive through the Layer 2 interface.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To add the tagged VLAN 100 to a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk allowed vlan add 100
```

To remove the tagged VLAN 100 from the interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk allowed vlan remove 100
```

See Also **interface, show vlan, switchport mode, switchport trunk native-vlan, switchport trunk tag native-vlan**

switchport trunk native-vlan

Sets native VLAN characteristics on a trunk port.

Synopsis **switchport trunk native-vlan** *vlan_id*

no switchport trunk native-vlan

Operands

vlan_id	Adds a VLAN to transmit and receive through the Layer 2 interface. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te)

Description Use this command to set the native VLAN characteristics of the Layer 2 trunk interface for classifying untagged traffic.

Usage Guidelines The native VLAN can be reset to the default setting using the **no switchport trunk native-vlan** command.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To set native VLAN characteristics for a VLAN whose VLAN id is 120:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk native-vlan 120
```

See Also **interface**, **show vlan**, **switchport mode**, **switchport trunk allowed vlan**, **switchport trunk tag native-vlan**

switchport trunk tag native-vlan

Enables tagging on native VLAN traffic.

Synopsis **switchport trunk tag native-vlan**

no switchport trunk tag native

Operands **None**

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to enable tagging for native traffic on a specific interface.

Usage Guidelines Use the **no switchport trunk tag native** command to untag native traffic for a specific interface.

Examples To enable tagging for native traffic on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk tag native-vlan
```

See Also **interface**, **show vlan**, **switchport mode**, **switchport trunk allowed vlan**, **switchport trunk native-vlan**

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 None

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 None

Examples To set the global system description specific to LLDP:

```
switch(conf-lldp)# system-description Brocade
```

See Also system-name

system-monitor

Specifies the FRUs on which the alert state and alert action is configured.

Synopsis

system-monitor {**fan** | **power** | **temp** | **cid-card** | **sfp** | **compact-flash** | **MM** | **LineCard** | **SFM**} **alert state** [**removed**] [**inserted**] [**on**] [**faulty**] | [**all**] | [**none**]

system-monitor {**fan** | **power** | **temp** | **cid-card** | **sfp** | **compact-flash** | **MM** | **LineCard** | **SFM**} **alert action** [**email**] [**raslog**] | [**all**] | [**none**]

system-monitor {**fan** | **power** | **temp** | **cid-card** | **sfp** | **compact-flash** | **MM** | **LineCard** | **SFM**} [**threshold** *down-threshold* {*integer*} *marginal-threshold* {*integer*}]

no system-monitor fan power alert state

no system-monitor fan power alert action

no system-monitor fan | **power threshold** *marginal-threshold*

no system-monitor fan | **power threshold** *down-threshold*

Operands

fan Configures fan settings.

power Configures power settings.

temp Displays the threshold for the temperature sensor component.

cid-card Displays the threshold for the CID card component.

sfp Displays the threshold for the small form factor pluggable (SFP) device.

compact-flash Displays the threshold for the compact flash device.

MM Displays the threshold for the management module.

LineCard Displays the threshold for the line card.

SFM Displays the threshold for the switch fabric module.

alert state removed | **inserted** | **on** | **faulty** | **all** | **none**
Configures one of the following FRU states to be monitored: removed, inserted, off, on, faulty, all, and none.

alert action email | **raslog**
Configures one of the alert actions for a specified FRU state. Fabric Watch generates action when there is a change in the FRU state. Supported alert actions are email and raslog.

temp | **compact-flash** Sets the policy parameters for calculating the overall status of the switch enclosure. The policy parameter values determine how many failed or faulty units of each contributor are allowed before triggering a status change in the switch from HEALTHY to MARGINAL or DOWN.

threshold *down-threshold integer*
Specifies the minimum number contributing to the DOWN status of the switch. A value of 0 indicates the down threshold is not used to calculate the overall threshold.

threshold *marginal-threshold integer*

Specifies the minimum number contributing to the MARGINAL status of the switch. A value of 0 indicates the down threshold is not used to calculate the overall threshold.

Default Factory thresholds are listed in Table 7.

TABLE 7 System-monitor factory thresholds

Component	Down threshold	Marginal threshold
Fan	2	1
Temperature sensor	2	1
Compact flash	1	0
Power supply	Platform-dependent	Platform-dependent

Command Modes Global configuration mode

Description Use this command to configure field-replaceable unit (FRU) states and actions. Based on these configuration settings, Fabric Watch generates action when there is a change in FRU state.

Usage Guidelines None

Examples

```
switch(config)# system-monitor ?
Possible completions:
  LineCard        Configure threshold and alert setting for component:LineCard
  MM              Configure threshold setting for component:MM
  SFM             Configure threshold setting for component:SFM
  cid-card        Configure threshold and alert setting for component:CID-CARD
  compact-flash   Configure threshold for component:COMPACT-FLASH
  fan             Configure threshold and alert setting for component:FAN
  power           Configure threshold and alert setting for component:
                  POWER SUPPLY
  sfp             Configure alert for component:SFP
  temp            Configure threshold for component:TEMPERATURE SENSOR

switch(config)# system-monitor sfm ?
Possible completions:
  threshold   Configure threshold for component:SFM

sw0(config)# system-monitor sfm threshold ?
Possible completions:
  down-threshold       Minimum number contributing to DOWN state of
                       component:SFM
  marginal-threshold   Minimum number contributing to MARGINAL state of
                       component:SFM

switch(config)# system-monitor sfm threshold down-threshold 3 marginal-threshold
2
switch(config)# system-monitor cid-card ?
Possible completions:
  alert       Configure alert for component:CID-CARD
  threshold   Configure threshold for component:CID-CARD

switch(config)# system-monitor cid-card alert ?
Possible completions:
```

```
  action   Action that may be taken when component:CID-CARD changes configured
           state
  state    Supported states for component:CID-CARD that may be monitored

switch(config)# system-monitor cid-card alert state ?
Possible completions:
  all  faulty  inserted  none  on  removed

switch(config)# system-monitor cid-card alert state faulty,inserted ?
Possible completions:
  action   Action that may be taken when component:CID-CARD changes configured
           state

switch(config)# system-monitor cid-card alert state faulty,inserted action ?
Possible completions:
  [raslog]  all  email  none  raslog

switch(config)# system-monitor cid-card alert state faulty,inserted action email
```

See Also show system monitor, system-monitor-mail

system-monitor-mail

Configures Fabric Watch e-mail alerts on the switch. For an e-mail alert to function correctly, add the IP addresses and host names to DNS in addition to configuring the domain name and name servers.

Synopsis **system-monitor-mail fru** *enable* | *email-id*

system-monitor-mail relay *host_ip* **|** *domain-name*

no system-monitor-mail fru

no system-monitor-mail relay *host_ip* | *domain-name*

Operands

fru	The FRU class for which alerts are configured.
enable	Enables or disables the e-mail alert.
email-id	Specifies the e-mail address to where the alert will be sent.
relay	Configures the relay host for email to work in a non-DNS environment.
host_ip	Specifies the IPv4 address of the mail server.
domain_name	Specifies the domain that corresponds to the email ID.

Default The default source is disabled.

Command Modes Global configuration mode

Description Use this command to configure Fabric Watch e-mail alerts on the switch.

Usage Guidelines Both relay parameters (the host IP and the domain name) must be configured in a non-DNS environment. In a DNS environment, only the host IP is required).

Example

```
switch(config)# system-monitor-mail ?
Possible completions:
  fru     Configure FRU mail settings
  relay   Configure relay ip mail settings

system-monitor-mail fru user1@brocade.com

system-monitor-mail fru user2@brocade.com

switch(config)# system-monitor-mail fru enable
switch(config- system-monitor-mail-fru/enable)# exit

switch(config)# system-monitor-mail relay ?
Possible completions:
  <host-ip:IP address>  <host-ip:string, min: 1 chars, max: 253 chars>

switch(config)# system-monitor-mail relay 1.2.3.4 ?
Possible completions:
  domain-name   Domain name server

switch(config)# system-monitor-mail relay 1.2.3.4 domain-name ?
Possible completions:
  <LINE:0-64>   Domain name[]
```

```
switch(config)# system-monitor-mail relay 1.2.3.4 domain-name  abc.brocade.com

switch# show running-config system-monitor-mail relay
system-monitor-mail relay 1.2.3.4 domain-name abc.brocade.com
```

To create a mapping:

```
switch(config)# system-monitor-mail relay host-ip 1.2.3.4 domain-name
englab.brocade.com
```

To delete the mapping:

```
switch(config)# no system-monitor-mail relay host-ip 1.2.3.4
```

To change the domain name:

```
switch(config)# system-monitor-mail relay host-ip 1.2.3.4 domain-name
mail.brocade.com
```

See Also system-monitor, show system monitor

system-name

Sets the global system name specific to LLDP.

Synopsis **system-name** *name*

no system-name

Operands

name	Specifies a system name for the LLDP. The valid value is a maximum of32 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 Use the **no system-name** command to delete the name.

Examples To specify a system name for the LLDP:

```
switch(conf-lldp)# system-name Brocade
```

See Also system-description

tacacs-server

Configures a Terminal Access Controller Access-Control System plus(TACACS+) server.

Synopsis **tacacs-server host** {*hostname* | *ip-address*} [**port** *portnum*] [**protocol** {**chap** | **pap**}] [**key** *shared_secret*] [**timeout** *secs*] [**retries** *num*]

no tacacs-server {*hostname* | *ip-address*}

Operands

host {*hostname* | *ip-address*}
Specifies the IP address or domain name of the TACACS+ server. IPv4 and IPv6 addresses are supported.

port *portnum*
Specifies the authentication port. The range is 0 through 65535. The default is 49.

protocol {*chap* | *pap*}
Specifies the authentication protocol. Options include CHAP and PAP. The default is CHAP.

key *shared_secret*
Specifies the text string that is used as the shared secret between the switch and the TACACS+ server to make the message exchange secure. The key must be between 8 and 40 characters in length. The default key is **sharedsecret**. The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the password in either double quotes or the escape character (\), for example **"secret!key"** or **secret\!key**.

timeout *secs*
Specifies the time to wait for the TACACS+ server to respond, in seconds. The default is 5 seconds.

retries *secs*
Specifies the number of attempts allowed to connect to a TACACS+ server. The default is 5 attempts.

Defaults Refer to the operand section.

Command Modes Global configuration mode

Description Use this command to configure attributes on the TACACS+ server. If a TACACS+ server with the specified IP address or host name does not exist, it is added to the server list. If the TACACS+ server already exists, this command modifies the configuration.

Usage Guidelines The **key** operand does not support an empty string.

Executing the **no** form of the **tacacs-server** command attributes resets the specified attributes to their default values.

Examples To configure an IPv4 TACACS+ server:

```
switch(config)# tacacs-server host 10.24.65.6 protocol chap retries 100
switch (config-tacacs-server-10.24.65.6)#
```

To modify an existing TACACS+ server configuration:

```
switch(config)# tacacs-server host 10.24.65.6
switch(config-tacacs-server-10.24.65.6)# key “changedsec”
```

To deletes the TACACS+ server:

```
switch(config)# no tacacs-server host 10.24.65.6
switch(config)# exit
```

```
switch# show running-config tacacs-server host
switch# show running-config tacacs-server host 10.xx.xx.xxx
tacacs-server host 10.xx.xx.xxx
key changedsec
```

To configure an IPv6 TACACS+ server:

```
switch(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010\ protocol
chap
switch(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010)# key "mysecret"
```

See Also radius-server, show running-config radius-server, show running-config tacacs-server

telnet

Establishes a Telnet session to a remote networking device.

Synopsis **telnet** {*IP Address* | *hostname*} [*port*]

Operands

IP Address	Specify the server IP address in IPv4 or IPv6 format.
hostname	Alternately, specify the host name, a string between 1 and 253 characters long
port	Specifies the port number in the remote device to connect to. The valid range is 0-65535. For the connection to succeed, a TCP server must be listening for client connections at this port. The default value for port number is 23.

Defaults By default, Telnet connects through port 23.

Command Modes Privileged EXEC mode

Description Use this command to establish a Telnet session from a switch to a remote networking device.

Usage Guidelines The following features are not supported:

- Display Telnet sessions
- Ability to terminate hung Telnet sessions

Examples To establish a Telnet session from a switch to a remote networking device.

```
switch# telnet 10.17.37.157
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.

Network OS (sw0)
sw0 login:
```

See Also ssh, **show running-config telnet server**, **show telnet server status**, **telnet server shutdown**

telnet server shutdown

Disables telnet service on the switch.

Synopsis **telnet server shutdown**

no telnet server shutdown

Operands None

Defaults None

Command Modes Global configuration mode

Description This command disables telnet service on the switch.

Usage Guidelines Use the **no telnet server shutdown** command to enable telnet service.

Examples None

See Also **show running-config telnet server**, **show telnet server status**, **telnet**

terminal

Sets terminal parameters for the current session.

Synopsis **terminal [length** *number_of_lines*]**[monitor][timeout** *value*]

no terminal [length][monitor][timeout]

Operands

length *number_of_lines*
Specifies the number of lines to be displayed. The range is 1 through 512. The default is 24. Specify 0 for infinite length.

monitor Enables terminal monitoring.

timeout *value* Specifies the timeout value in minutes. The range is 0 through 136. Specify 0 to disable timeout.

Defaults Refer to the operand descriptions.

Command Modes Privileged EXEC mode

Description Use this command to control terminal parameters for the current session. This command overrides the timeout configuration set by the **line vty exec-timeout** command, but only for the duration of the current session. When the current session ends, the configured values apply for any subsequent sessions.

Use the **no terminal** command (optionally with a specified operand) to restore the current terminal settings to default.

Usage Guidelines Press the space bar to display the next page.

This command is supported only on the local switch.

This command is not available on the standby management module.

Examples To set the display length to 30 lines:

```
switch# terminal length 30
```

To set the timeout length to 60 minutes:

```
switch# terminal timeout 60
```

To restore all settings to default values:

```
switch# no terminal
```

To restore only the timeout setting to its default values:

```
switch# no terminal timeout
```

See Also line vty exec-timeout

threshold-monitor cpu

System Monitor monitors CPU usage of the system and alerts the user when configured thresholds are exceeded.

Synopsis **threshold-monitor cpu poll** *polling_interval* **retry** *number_of_retries* **limit** *limit-usage*

no threshold-monitor cpu

Operands

poll	Specifies the polling interval (in seconds).
polling_interval	The time in seconds after which the system monitor will poll the resource usage.
retry	Specifies the system monitor's number of retries.
number_of_retries	The number of retries that the system monitor takes before triggering an action.
limit	Specifies the default CPU limit. When the limit is exceeded, the system monitor sends a RASlog WARNING message. When the usage returns below the limit, System Monitor sends a RASlog INFO message. Valid values range between 0 to 80 percent.
limit-usage	The usage limit as a percentage of available resources.

Defaults Table 8 lists the factory defaults for memory thresholds

TABLE 8 Factory defaults for memory threshold monitoring

Operand	Memory
Poll	120 seconds
Retry	3
Limit	75%

Command Modes Global configuration mode

Description Use this command to monitor CPU usage of the system and alert the user when configured thresholds are exceeded

Usage Guidelines None

Examples

```
switch(config)# threshold-monitor ?
Possible completions:
Cpu           Configure settings for component:CPU
Memory        Configure settings for component:MEMORY
interface     Monitor Interface class
security      Monitor security class
sfp           Monitor SFP class
```

```
switch(config)# threshold-monitor cpu
Possible completions:
  actions   Action to be taken when usage exceeds limit
  limit     PERCENT:0-80 Percent threshold usage for component:CPU
  poll      NUMBER:10-3600 Polling interval
  retry     NUMBER:1-100 Number of retries

switch(config)# threshold-monitor cpu actions raslog limit 60 ?
Possible completions:
  poll    NUMBER:10-3600 Polling interval
  retry   NUMBER:1-100 Number of retries

switch(config)# threshold-monitor cpu actions raslog limit 60 poll ?
Possible completions:
  <NUMBER:10-3600 Polling interval in secs after which CPU sample be taken>[120]

switch(config)# threshold-monitor cpu actions raslog limit 60 poll 30 ?
Possible completions:
  retry   NUMBER:1-100 Number of retries

switch(config)# threshold-monitor cpu actions raslog limit 60 poll 30 retry 2
switch(config)# threshold-monitor memory ?
Possible completions:
  actions      Action to be taken when usage exceeds limit
  high-limit   PERCENT:0-80 : Percent high threshold usage for component:MEMORY
  limit        PERCENT:0-80 : Percent threshold usage for component:MEMORY
  low-limit    PERCENT:0-80 : Percent low threshold usage for component:MEMORY
  poll         Polling interval
  retry        NUMBER:0-100: Number of retries for component:MEMORY

switch(config)# threshold-monitor memory actions none high-limit ?
Possible completions:
  <PERCENT:0-80 Limit when reached
desired action be taken>[70]

switch(config)# threshold-monitor memory actions none high-limit 80 low-limit 50
limit 70 ?
Possible completions:
  poll    Polling interval
  retry   NUMBER:0-100: Number of retries for component:MEMORY>

switch(config)# threshold-monitor memory actions none high-limit 80 low-limit 50
limit 70 retry 2 poll ?
Possible completions:
  <NUMBER:0-3600 Polling interval in secs>[120]

switch(config)# threshold-monitor memory actions none high-limit 80 low-limit 50
limit 70 retry 2 poll 30
```

See Also system-monitor, show system monitor

threshold-monitor interface

System Monitor monitors port statistics on all external Gigabit Ethernet interfaces: 1 Gb, 10 Gb, and 40 Gb. When any monitored error crosses the configured high or low threshold, an alert is generated.

Synopsis **threshold-monitor interface policy** *policy_name* **type [CRCAlignErrors | SymbolErrors | IFG | MissingTerminationCharacter]**

[threshold [high-threshold|low_threshold|buffer]

[above [highthresh-action raslog | fence | both | none]

[below [highthresh-action raslog | fence | both | none]

[[above [lowthresh-action raslog | fence | both | none] [below [lowthresh-action raslog | fence | both | none]]

timebase [day|hour|minute|none] *value*

no threshold-monitor interface

Operands

policy	Specifies whether the system will monitor interface parameters using the default configuration or custom settings.
custom	Specifies a custom policy configuration that can be saved and applied using the **apply** command.
default	Assumes the interface default values.
type	Specifies the Interface type. Possible completions are as follows:
CRCAlignErrors	The total number of frames received with either a bad Frame Check Sequence (FCS) or an alignment error.
SymbolErrors	The number of words received as an unknown (invalid) symbol. Large symbol errors indicate a bad device, cable, or hardware.
IFG	The minimum-length interframe gap (IFG) between successive frames is violated. The typical minimum IFG is 12 bytes.
Missing Termination Character	The number of frames that terminated by anything other than the Terminate character.
actions	Specifies the alert notification method.
raslog	Specifies RASlog as the action System Monitor triggers.
fence	Specifies Port Fence as the action System Monitor triggers. Port Fencing is applicable only to the IFG error.
both	Specifies both RASlog and Port Fence as actions System Monitor triggers.
none	Specifies none (no alert notification).
threshold	Specifies the values for high, low, and buffer threshold values. These values are used as thresholds to trigger different alerts.

alert Specifies the type of threshold.

- **High threshold** specifies the higher limit for Interface errors.
- **Low threshold** specifies the lower limit for Interface errors.
- **Above high threshold** specifies the action for crossing the high threshold.
- **Above low threshold** specifies the action for crossing the low threshold.
- **Below high threshold** specifies the action for Security violations to be below the high threshold.
- **Below low threshold** specifies the action for Security violations to be below the low threshold.
- **In-Range** specifies the value of an error on a configured interface that is in the buffer range. The buffer value cannot exceed the average of the high and low threshold value.

timebase Determines if the allotted amount of time has passed since the previous reading. Polling values are taken at different intervals depending on the configured time base.

Defaults None

Command Modes Global configuration mode

Description Use this command to configure high and low thresholds against which login failures are compared. Based on the configuration settings, System Monitor generates a RASlog action.

Usage Guidelines None

Examples

```
switch(config)# threshold-monitor interface
Possible completions:
  apply    Apply configuration
  pause    Pause monitoring
  policy

switch(config)# threshold-monitor interface  policy custom type Ethernet area
Possible completions:
  MissingTerminationCharacters
                              Frames that terminated by anything other than the
                              Terminate character.
  CRCAlignErrors              Frames received with CRC and/or Align Errors
  IFG                         Number of times Inter Frame Gap was violated
  SymbolErrors                Number of words received as unknown symbol

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors
Possible completions:
  alert       Alert configuration
  threshold   Threshold configuration

switch(config)# threshold-monitor interface policy  custom type Ethernet area
CRCAlignErrors threshold
Possible completions:
  buffer           Buffer threshold value
  high-threshold   High threshold value
  low-threshold    Low threshold value
  timebase         Configure timebase for monitoring
```

```
switch(config)# threshold-monitor interfacepolicy  custom type Ethernet area
CRCAlignErrors threshold
Possible completions:
  buffer           Buffer threshold value
  high-threshold   High threshold value
  low-threshold    Low threshold value
  timebase         Configure timebase for monitoring

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors threshold high-threshold ?
Possible completions:
  <int>[20]

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors threshold high-threshold 80
Possible completions:
  buffer          Buffer threshold value
  low-threshold   Low threshold value
  timebase        Configure timebase for monitoring

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors threshold high-threshold 80 low-threshold ?
Possible completions:
  <int>[1]

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors threshold high-threshold 80 low-threshold 10
Possible completions:
  buffer     Buffer threshold value
  timebase   Configure timebase for monitoring

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors threshold high-threshold 80 low-threshold 10 buffer ?
Possible completions:
  <int>[5]

switch(config)# threshold-monitor interface policy custom type Ethernet area
CRCAlignErrors threshold high-threshold 80 low-threshold 10 buffer 10 timebase
Possible completions:
  day  hour  minute  none

switch(config)# threshold-monitor interface  policy custom type Ethernet area
CRCAlignErrors threshold high-threshold 80 low-threshold 10 buffer 10 timebase
hour
switch(config)#

switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
Possible completions:
  alert       Alert configuration
  threshold   Threshold configuration

switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
alert
Possible completions:
  above  Above trigger
  below  Below trigger
```

```
switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
alert above
Possible completions:
  highthresh-action  lowthresh-action

switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
alert above highthresh-action
Possible completions:
  all none  fence  raslog

switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
alert above highthresh-action fence,raslog lowthresh-action
Possible completions:
  all none  raslog

switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
alert above highthresh-action fence,raslog lowthresh-action
Possible completions:
  all none  raslog

switch(config)# threshold-monitor interface policy custom type Ethernet area IFG
alert above highthresh-action fence,raslog lowthresh-action email raslog
```

threshold-monitor memory

System Monitor monitors memory usage of the system and alerts the user when configured thresholds are exceeded.

Synopsis **threshold-monitor memory poll** *polling_interval* **retry** *number_of_retries* **limit** *limit-usage* **action** {**raslog** | **none**} **high-limit** *high-limit-usage* **low-limit** *low-limit-usage*

no threshold-monitor memory

Operands

poll	Specifies the polling interval (in seconds).
polling_interval	The time in seconds after which the system monitor will poll the resource usage.
retry	Specifies the system monitor's number of retries.
number_of_retries	The number of retries that the system monitor takes before triggering an action.
limit	Specifies the default CPU limit. When the limit is exceeded, the system monitor sends a RASlog WARNING message. When the usage returns below the limit, System Monitor sends a RASlog INFO message. Valid values range between 0 to 80 percent.
limit-usage	The usage limit as a percentage of available resources.
action	Specifies the action the system monitor triggers. Valid action types are RASlog and None.
raslog|**none**	The specified action the system monitor triggers when a threshold is crossed.
high-limit	Specifies an upper usage limit for memory as percentage of available memory. This value must be greater than the value set by the -limit parameter. The maximum is 90 percent. When memory usage exceeds this limit, System Monitor generates a CRITICAL RASlog message. The default is 80 percent.
high-limit-usage	The upper usage limit for memory as a percentage of available memory.
low-limit	Specifies a lower usage limit for memory as percentage of available memory. This value must be smaller than the value set by the -limit parameter. When memory usage exceeds or falls below this limit, the system monitor generates an INFO RASlog message. The default for all platforms is 50 percent.
low-limit-usage	The lower usage limit for memory as a percentage of available memory.

Default Table 8 lists the factory defaults for memory thresholds

TABLE 9 Factory defaults for memory threshold monitoring

Operand	Memory
Low-limit	40%

TABLE 9 Factory defaults for memory threshold monitoring

Limit	60%
High-limit	70%
Poll	120 seconds
Retry	3
Action	None

Command Modes Global configuration mode

Description Use this command to monitor memory usage of the system and alert the user when configured thresholds are exceeded.

Usage Guidelines None

Examples

```
switch(config)# threshold-monitor Memory ?
Possible completions:
  actions      Action to be taken when usage exceeds limit
  high-limit   PERCENT:0-80 : Percent high threshold usage for component:MEMORY
  limit        PERCENT:0-80 : Percent threshold usage for component:MEMORY
  low-limit    PERCENT:0-80 : Percent low threshold usage for component:MEMORY
  poll         Polling interval
  retry        NUMBER:0-100: Number of retries for component:MEMORY

switch(config)# threshold-monitor Memory actions none high-limit ?
Possible completions:
  <PERCENT:0-80 Limit when reached
desired action be taken>[70]

switch(config)# threshold-monitor Memory actions none high-limit 80 low-limit
50 ?
Possible completions:
  limit   PERCENT:0-80 : Percent threshold usage for component:MEMORY
  poll    Polling interval
  retry   NUMBER:0-100: Number of retries for component:MEMORY

switch(config)# threshold-monitor Memory actions none high-limit 80 low-limit 50
limit 70 retry 2 poll ?
Possible completions:
  <NUMBER:0-3600 Polling interval in secs>[120]

switch(config)# threshold-monitor Memory actions none high-limit 80 low-limit 50
limit 70 retry 2 poll 30
```

See Also system-monitor, show system monitor

threshold-monitor security

System Monitor monitors the system's security parameters. Supported Security areas are Telnet Violation and Login Violation.

Synopsis **threshold-monitor security policy** *policy_name* **area [telnet-violation | login-violation] alert [above [highthresh-action all | raslog | none] [below [highthresh-action all | raslog | none] [lowthresh-action all |raslog|none]]]**

no threshold-monitor security

Operands

policy		Specifies whether the system will monitor Security parameters using the default configuration or custom settings.
	custom	Specifies a custom policy configuration that can be saved and applied using the **apply** command.
	default	Assumes the Security default values listed in Table 10.
action		Specifies the threshold values.
	alert	**High threshold** specifies the higher limit for Security violations. **Low threshold** specifies the lower limit for Security violations. **Above high threshold** specifies the action for crossing the high threshold. **Below high threshold** specifies the action for Security violations to be below the high threshold. **Below low threshold** specifies the action for Security violations to be below the low threshold.
buffer		Specifies the buffer value for in-range behavior.
	buffer_value	Defines a zone within which event criteria are met, rather than a single threshold value.
timebase		Determines if the allotted amount of time has passed since the previous reading. Polling values are taken at different intervals depending on the configured time base.

Defaults

TABLE 10 Security area default settings

Area	High threshold	Low threshold	Buffer	Timebase
Telnet Violation	2	1	0	Minute
Login Violation	2	1	0	Minute

Command Modes Global configuration mode

Description Use this command to configure high and low thresholds against which login failures are compared. Based on the configuration settings, System Monitor generates a RASlog action.

Usage Guidelines None

Examples

```
switch(config)# threshold-monitor ?
Possible completions:

Cpu           Configure settings for component:CPU
Memory        Configure settings for component:MEMORY
interface     Monitor Interface class
security      Monitor security class
sfp           Monitor SFP class

switch(config)# threshold-monitor security ?
Possible completions:
  apply    Apply configuration
    policy
  area   Security Areas

switch(config)# threshold-monitor security policy custom area ?
Possible completions:
  login-violation    Security Area login violation
  telnet-violation   Security Area telnet violation

switch(config)# threshold-monitor security policy custom area-monitor-environment
securitymonitor area telnet-violation ?
Possible completions:
  alert                Alert configuration
  threshold            Threshold configuration
  timebase             Configure timebase for monitoring

switch(config)# threshold-monitor security policy custom area telnet-violation
threshold ?
Possible completions:
  buffer           Buffer threshold value
  high-threshold   High threshold value
  low-threshold    Low threshold value

switch(config)# threshold-monitor security policy custom area telnet-violation
threshold high-threshold 10 buffer 3

switch(config)# threshold-monitor security policy custom area telnet-violation
timebase hour
```

threshold-monitor sfp

System Monitor monitors the system's SFP parameters.

Synopsis **threshold-monitor sfp policy** *policy_type* **type** *type* **area** *SFP_area* **action** [**alert** [**above highthresh-action**] [**below highthresh-action**] [**below lowthresh-action**]] **buffer** *buffer_value*

no threshold-monitor sfp

Operands

policy	Specifies whether the system will monitor SFP parameters using the default configuration or custom settings.
custom	Specifies a custom policy configuration that can be saved and applied using the **apply** command.
default	Assumes the SFP type and SFP area default values listed in Table 11.
type	Specifies the SFP type. Possible completions are as follows:
1GLR	— SFP type 1GLR
1GSR	— SFP type 1GSR
10GER	— SFP type 10GER
10GLR	— SFP type 10GLR
10GSR	— SFP type 10GSR
10GUSR	— SFP type 10GUSR
QSFP	— SFP type QSFP
area	Specifies one of the following SFP parameters to be monitored.
RXP	Measures the amount of incoming laser, in uWatts.
TXP	Measures the amount of outgoing laser, in uWatts.
Temperature	Measures the physical temperature of the SFP, in degrees Celsius.
Current	Measures the amount of supplied current to the SFP transceiver.
Voltage	Measures the amount of voltage supplied to the SFP.
action	Specifies the threshold values
alert	High threshold specifies the higher limit for SFP parameter values. Low threshold specifies the lower limit for SFP parameter values. Above high threshold specifies the action for crossing the high threshold. Below high threshold specifies the action for SFP parameter values to be below the high threshold. Below low threshold specifies the action for SFP parameter values to be below the low threshold.
buffer	Specifies the buffer value for in-range behavior.
buffer_value	Defines a zone within which event criteria are met, rather than a single threshold value.

Defaults SFP types and area defaults are listed in Table 11.

TABLE 11 SFP types and SFP area defaults

SfpType	Area	Default Value	
1 GSR	Temperature (Centigrade)	100	-40
	Voltage (mVoltage)	3600	3000
	RXP (uW)	1122	8
	TXP (uW)	1000	60
	Current (mAmp)	12	2
1 GLR	Temperature (Centigrade)	90	-45
	Voltage (mVoltage)	3700	2900
	RXP (uW)	501	6
	TXP (uW)	794	71
	Current (mAmp)	45	1
10 GSR	Temperature (Centigrade)	90	-5
	Voltage (mVoltage)	3600	3000
	RXP (uW)	1000	32
	TXP (uW)	794	251
	Current (mAmp)	11	4
10 GLR	Temperature (Centigrade)	88	-5
	Voltage (mVoltage)	3600	2970
	RXP (uW)	1995	16
	TXP (uW)	1585	158
	Current (mAmp)	85	15
10GUSR	Temperature (Centigrade)	100	-5
	Voltage (mVoltage)	3600	2970
	RXP (uW)	2000	32
	TXP (uW)	2000	126
	Current (mAmp)	11	3
QSFP	Temperature (Centigrade)	75	-5
	Voltage (mVoltage)	3600	2970
	RXP (uW)	1995	40
	TXP (uW)	0	0
	Current (mAmp)	10	1

Command Modes Global configuration mode

Description Use this command to monitor SFP parameters and alert the user when configured thresholds are exceeded.

Usage Guidelines None

Examples

```
switch(config)# threshold-monitor ?
Possible completions:

Cpu           Configure settings for component:CPU
Memory        Configure settings for component:MEMORY
interface     Monitor Interface class
security      Monitor security class
sfp           Monitor SFP class

switch(config)# threshold-monitor sfp policy custom ?
Possible completions:
  type

switch(config)# threshold-monitor sfp policy custom type ?

Possible completions:
  1GLR      SFP type 1GLR
  1GSR      SFP type 1GSR
  10GER     SFP type 10GER
  10GLR     SFP type 10GLR
  10GSR     SFP type 10GSR
  10GUSR    SFP type 10GUSR
  QSFP      SFP type QSFP

switch(config)# threshold-monitor sfp policy custom type QSFP ?
Possible completions:
  area   SFP Areas

switch(config)# threshold-monitor sfp policy custom type QSFP area ?
Possible completions:
  rxp           SFP Area RXP
  txp           SFP Area TXP
  current       SFP Area Current
  temperature   SFP Area Temperature
  voltage       SFP Area Voltage

switch(config)# threshold-monitor sfp policy custom type QSFP area rxp ?
Possible completions:
  alert                 Alert configuration
  threshold             Threshold configuration

switch(config)# threshold-monitor sfp custom type QSFP area rxp threshold ?
Possible completions:
  buffer           Buffer threshold value
  high-threshold   High threshold value
  low-threshold    Low threshold value

switch(config)# threshold-monitor sfp custom type QSFP area rxp threshold
high-threshold 2000 low-threshold 1000
```

timers

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) throttle timers.

Synopsis **timers** {**lsa-group-pacing** *interval* | **throttle spf** *start hold max*}

Operands

lsa-group-pacing *interval*	Specifies the interval (in seconds) at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged by the OSPF process. The default is 240. The range is 10 to 1800.
throttle spf	Specifies start, hold and maximum wait intervals for throttling SPF calculations for performance. The values you enter are in milliseconds.
start	Initial SPF calculation delay. The default is 0. The range is 0 to 60000.
hold	Minimum hold time between two consecutive SPF calculations. The default is 5000. The range is 0 to 60000.
max	Maximum wait time between two consecutive SPF calculations. The default is 10000. The range is 0 to 60000.

Default Defaults for the options are listed above.

Command Modes Router configuration mode.

Description Configures LSA pacing and SPF throttle timers.

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

Usage Guidelines The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance. To restore the pacing interval to its default value, enter the **no timers lsa-group-pacing** command.

To set the SPF timers back to their defaults, run the **no timers throttle spf** command.

Examples To set the LSA group pacing interval to 30 seconds:

```
Switch(conf-ospf-router)# timers lsa-group-pacing 30
```

To change the SPF delay to 10000 milliseconds, the hold time to 15000 milliseconds, and the maximum wait time to 30000 milliseconds:

```
Switch(conf-ospf-router)# timers throttle spf 10000 15000 30000
```

traceroute

Traces the network path of packets as they are forwarded to a destination address.

Synopsis **traceroute** *dest-addr* [**src-addr** *src-addr*] | [**ipv6** *dest-ipv6-addr*] | *host-name* [**maxttl** *value*] [**minttl** *value*] [**timeout** *seconds*]

Operands

dest-addr	Specifies the IPv4 address of the destination device.
src-addr *address*	Specifies the IPv4 address of the source device.
ipv6 *dest-ipv6-addr*	Specifies the IPv6 address of the destination device. This operand is valid only with the **ping** command.
maxttl *value*	Maximum Time To Live value in a number of hops.
minttl *value*	Minimum Time To Live value in a number of hops.
timeout *seconds*	The traceroute timeout value.

Defaults There is no default for this command.

Command Modes Privileged EXEC mode

Description Use this command to trace the network routes from a source address to a specified destination address.

Usage Guidelines None

Examples To execute an IPv4 traceroute.

```
switch# traceroute 172.16.4.80
traceroute to 172.16.4.80 (172.16.4.80), 64 hops max
 1   10.24.80.1 (10.24.80.1) 0.588ms 0.139ms 0.527ms
 2   10.31.20.61 (10.31.20.61) 0.550ms 0.254ms 0.234ms
 3   10.16.200.113 (10.16.200.113) 0.408ms 0.285ms 0.282ms
 4   10.110.111.202 (10.110.111.202) 5.649ms 0.283ms 0.288ms
 5   10.130.111.38 (10.130.111.38) 1.108ms 0.712ms 0.704ms
 6   10.192.0.42 (10.192.0.42) 37.053ms 32.985ms 41.744ms
 7   172.16.56.10 (172.16.56.10) 33.110ms 33.349ms 33.114ms
 8   172.16.4.9 (172.16.4.9) 34.096ms 33.023ms 33.122ms
 9   172.16.4.80 (172.16.4.80) 76.702ms 83.293ms 79.570ms
```

To execute an IPv6 traceroute, with minimum and maximum TTL values.

```
switch# traceroute ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 maxttl 128 minttl
30 src-addr fec0:60:69bc:92:205:33ff:fe9e:3f20 timeout 3
traceroute to fec0:60:69bc:92:218:8bff:fe40:1470
(fec0:60:69bc:92:218:8bff:fe40:1470), 128 hops max, 80 byte packets
30  fec0:60:69bc:92:218:8bff:fe40:1470
(fec0:60:69bc:92:218:8bff:fe40:1470)  2.145 ms  2.118 ms  2.085 ms
```

See Also ping

track

Specifies an interface to track.

Synopsis **track** {**FortyGigabitEthernet** *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **Port-channel** *number* | **TenGigabitEthernet** *rbridge-id/slot/port*} [**priority** *range*]

no track {**FortyGigabitEthernet** *rbridge-id/slot/port* | **GigabitEthernet** *rbridge-id/slot/port* | **Port-channel** *number* | **TenGigabitEthernet** *rbridge-id/slot/port*} [**priority** *range*]

Operands

FortyGigabitEthernet *rbridge-id/slot/port*	Specifies a valid 40-Gbps port interface.
rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
GigabitEthernet	Specifies a valid 1-Gbps Ethernet interface
rbridge-id	Specifies the ID of the routing bridge.
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 1 through 6144.
TenGigabitEthernet	Specifies a valid 10-Gbps Ethernet interface.
rbridge-id	Specifies the ID of the routing bridge.
slot	Specifies a valid slot number.
port	Specifies a valid port number.
priority *range*	The track priority is a number from 1 to 254 to use when the tracked interface up or down event is detected. For VRRP, if the tracked interface becomes disabled, the current router priority is reduced *to* the track-port priority, (For VRRP only, interface tracking does not have any effect on an owner router; the owner priority can not be changed from 255.) For VRRP-E, if the tracked interface becomes disabled, the current router priority is reduced *by* the track-port priority,

Default Default priority range is 2.

Command Modes Virtual-router-group configuration mode.

Description Specifies the interface to track. For VRRP, the tracked interface can be any tengigabitethernet, fortygigabitethernet, gigabitethernet, or port-channel interface other than the one on which this command is issued.

The maximum number of interfaces you can track per virtual router is 16.

Usage Guidelines Use the **no** parameter with this command to remove the tracked port configuration. This command can be used for VRRP or VRRP-E.

Examples To set the track port to 21/2/4 and the track priority to 60:

```
switch(config)# rbridge-id 21
switch(config-rbridge-id-21)# protocol vrrp
switch(config-rbridge-id-21)# int te 21/1/6
switch(conf-if-te-21/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# track tengigabitethernet 21/2/4 priority 60
```

See Also vrrp-group

transmit-holdcount

Configures the maximum number of Bridge Protocol Data Units (BPDUs) transmitted per second for the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), and R-PVST+.

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 value 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 Brocade Network OS v3.0.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples To change the number of BPDUs transmitted to 3 seconds:

```
switch(conf-mstp)# transmit-holdcount 3
```

See Also show spanning-tree mst detail

trunk-enable

Enables trunking on a Fibre Channel port.

Synopsis **trunk-enable**

no trunk-enable

Operands None

Defaults By default, trunking is disabled.

Command Modes Interface Fibre Channel configuration submode

Description Use this command to enable trunking on a Fibre Channel port.

Use the **no** version of this command to disable trunking on a Fibre Channel port.

Usage Guidelines This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

A long distance link can also be configured to be part of a trunk group.

While using R_RDY mode flow control, an E_Port cannot form trunk groups of long distance links even if trunking is enabled.

Examples To enable trunking mode on a Fibre Channel port:

```
switch (config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# trunk-enable
```

To disable trunking mode on a Fibre Channel port:

```
switch (config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# no trunk-enable
```

See Also **desire-distance, fill-word, interface, isl-r_rdy, long-distance,** show running-config interface FibreChannel**, shutdown, speed (Fibre Channel), vc-link-init**

unhide fips

Makes available irreversible commands used in enabling FIPS compliance.

Synopsis **unhide fips**

Operands None

Defaults By default, irreversible commands related to enabling FIPS compliance are hidden.

Command Modes Privileged EXEC mode.

Description This command makes the following hidden commands available: **prom-access disable**, **fips root disable**, **fips selftests**, and **fips zeroize**.

Usage Guidelines Enter "**fibranne**" at the Password prompt to run the command.

This command applies only in the standalone mode. This command can be entered only from a user account with the admin role assigned.

Examples To make available all irreversible commands using in enabling FIP compliance:

```
switch# unhide fips
Password: *****
```

See Also fips root disable, fips selftests, fips zeroize, prom-access disable, show fips

unlock username

Unlocks a locked user account.

Synopsis **unlock username** *name*

Operands

name	The name of the user account.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to unlock a user who has been locked out because of unsuccessful login attempts. A user account is locked by the system when the configured threshold for login retires has been reached.

Usage Guidelines None

Examples The following example unlocks a user account:

```
switch# unlock username testUser
Result: Unlocking the user account is successful
```

See Also show running-config username, show users, username, unlock username

usb

Enables or disables an attached USB device.

Synopsis **usb** {**on** |**off**} [**rbridge-id** *rbridge-id]*

Operands **rbridge-id** *rbridge-id* Executes the command on a switch specified by its Rbridge ID.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable an attached USB device. The device will be inaccessible until it is enabled.

Usage Guidelines A switch reload will automatically turn the USB device off.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples To enable a USB device attached to the local switch:

```
switch# usb on
USB storage enabled
```

To disable a USB device attached to the local switch:

```
switch# usb off
USB storage disabled
```

See Also usb dir, usb remove

usb dir

Lists the contents of an attached USB device.

Synopsis **usb dir** [**rbridge-id** *rbridge-id]*

Operands **rbridge-id** *rbridge-id* Executes the command on a switch specified by its Rbridge 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.

This command is supported only on the local switch.

This command is not supported on the standby management module.

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, usb remove

usb remove

Removes a file from an attached USB device.

Synopsis **usb remove directory** *directory* **file** *file* [**rbridge-id** *rbridge-id*]

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.
rbridge-id *rbridge-id*	Executes the command on a switch specified by its Rbridge 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.

This command is supported only on the local switch.

This command is not supported on the standby management module.

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, usb dir

username

Configures a user account.

Synopsis **username** *username* **password** *password* **role** *role_name* [**encryption-level** {**0** | **7**}] [**desc** *description*] [**enable true** | **false**]

no username *name*

Operands

username	Specifies the account login name.
password *password*	Specifies the account password. The exclamation mark (!) is supported, and you can specify the password in either double quotes or the escape character (\), for example **"secret!password"** or **secret\!password.**
role *role_name*	Specifies the role assigned to the user account. The role is optional and, by default, the user's role is read-only.
encryption-level {**0** | **7**}	Specifies the password encryption level. The values are 0 (clear text) and 7 (encrypted). Clear text (0) is the default.
desc *description*	Specifies a description of the account (optional). The description can be up to 64 characters long, and can include any printable ASCII character, except for the following characters: single quotation marks (‘), double quotation marks(“), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces. you must enclose the text in double quotation marks.
enable true | **false**	Specifies whether the account is enabled or disabled. A user whose account is disabled cannot login. The default account status is enabled.

Defaults The default account status is enabled (enable = true).

The default role has read-only access permissions.

Command Modes Global configuration mode

Description Use this command to assign attributes for a user.

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.

All active login sessions for a user are terminated if the user's password or role is changed.

Examples To configure a user account:

```
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)#
```

To modify an existing user account:

```
switch(config)# username testUser enabled false
switch(config-username-testUser)# desc “add op test user”
switch(config)# no username testUser desc
```

See Also show running-config username, show users, unlock username

vc-link-init

Specifies the fill word used on long distance links for an 8 Gbps Fibre Channel port.

Synopsis **vc-link-init** {**idle** | **arb**}

Operands

idle	Sets the long distance link fill word to IDLE.
arb	Sets the long distance link fill word to ARB(ff).

Defaults The default value is **idle**.

Command Modes Interface Fibre Channel configuration submode

Description Use this command to specify the fill word used in long distance links. It must be set to the same value as the fill word configured for the remote port. Therefore, if the remote port link initialization and fill word combination is **idle-idle**, then the fill word for the long distance link must be set to **idle**. If the remote port link initialization/fill word combination is set to **arbff-arbff**, **idle-arbff**, or **aa-then-ia**, then the fill word for the long distance link must be set to **arb**.

Usage Guidelines This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6730-32 and Brocade VDX 6730-76 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples To set the fill word for a long distance link:

```
switch (config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# vc-link-init arb
```

See Also **desire-distance**, **fill-word**, **interface**, **isl-r_rdy**, **long-distance**, **show running-config interface FibreChannel**, **shutdown**, **speed (Fibre Channel)**, **trunk-enable**

vcenter

Authentication with the vCenter must occur before any discovery transactions are initiated. In order to authenticate with a specific vCenter, you must configure the URL, login, and password properties on the VDX switch.

Synopsis **vcenter**

vcenter MYVC interval

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to authenticate with a vCenter.

Usage Guidelines None

Example

```
switch(config)# vcenter MYVC url https://10.2.2.2 username user password pass
switch(config)# vcenter MYVC activate
switch(config)# no vcenter MYCV activate
switch(config)# no vcenter MYVC
```

See Also show port-profile, show vnetwork

VCS

Configures Brocade VCS Fabric technology parameters.

Synopsis **vcs [rbridge-id** *rbridge-id*] **[vcsId** *ID*] [**enable** *ID*]

no vcs enable

Operands

rbridge-id *rbridge-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.
vcsId *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 *ID*	Enables Brocade VCS Fabric mode.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to configure the Brocade VCS Fabric parameters (VCS ID and the switch RBridge ID) and to enable Brocade VCS Fabric mode. You can set the Brocade VCS Fabric parameters and enable Brocade VCS Fabric mode at the same time, or you can enable Brocade VCS Fabric 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 Brocade VCS Fabric mode.

Usage Guidelines Each time you change the Brocade 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 Brocade VCS Fabric commands.

- vcs enable
- no vcs enable
- vcs rbridge-id # enable
- vcs vcsId # enable
- vcs vcsID # rbridge-id # enable

Examples Enable the Brocade VCS Fabric by entering one of the following commands, based on your current configuration.

- If the Brocade VCS Fabric is already disabled:

Command	Command Behavior
`vcs enable`	The RBridge ID is not changed, the VCS ID becomes 1, and Brocade VCS FabricBrocade VCS Fabric mode is enabled.
`vcs vcsid` *x* `rbridge-id` *y* `enable`	The RBridge ID is changed, the VCS ID is changed, and Brocade VCS Fabric mode is enabled.
`vcs vcsid` *x* `enable`	The RBridge ID is not changed, the VCS ID is changed, and Brocade VCS Fabric mode is enabled.
`vcs rbridge-id y enable`	The RBridge is changed, the VCS ID becomes 1, and Brocade VCS Fabric mode is enabled.

- If the Brocade VCS Fabric is already enabled:

`no vcs enable`	The RBridge ID is set to 1, the VCS ID is set to 0, and VCS is disabled.
`vcs vcsid x rbridge-id y`	The VCS ID is changed and the RBridge ID is changed.
`vcs vcsid x`	Changes the VCS ID.

See Also **show vcs**

vcs virtual ip

Assigns a single virtual IP address to all switches in a Brocade VCS Fabric.

Synopsis **vcs virtual-ip address** *ipv4_address/prefix_len*

no vcs virtual-ip address

Operands *ip address* Configures the virtual IP address.

ipv4_address/prefix_len
Specifies the IP address in IPv4 format using a prefix.

Defaults None

Command Modes Global configuration mode

Description Use this command to assign a single virtual IP address to the configured principal switch. When you configure the virtual IP address is configured for the first time, the address is assigned to the principal switch. You can then access the principal switch through the management port IP address or the virtual IP address. The virtual IP configuration is global in nature. All the nodes in the fabric will be configured with the same virtual IP address, but the address is always bound to the current Principal switch.

The **no vcs virtual-ip address** removes the currently-configured virtual IP address.

Usage Guidelines This command can be used in VCS fabric mode only after the fabric has formed successfully. The virtual IP address cannot be configured on a standalone node.

The command can be executed from any node. However, you cannot remove a virtual IP address when you are logged on to the switch using the virtual IP address. Use the management port IP address or the serial console to configure the virtual IP address.

It is the responsibility of Network Administrator to ensure that the virtual IP address assigned is not a duplicate of address assigned to any other management port in the VCS fabric.

The virtual IP address should be configured on the same subnet as the management interface IP address.

Examples To assign a virtual IP address to the principal switch and verify the operation:

```
switch(config)# vcs virtual ip address 10.21.87.2/20
switch(config)# do show vcs virtual-ip
Virtual IP              :10.21.87.2/20
Associated rbridge-id   : 2
```

To remove the currently configured virtual IP address:

```
switch(config)# vcs virtual ip address
```

See Also **show vcs**

virtual-fabric

Designates the Virtual Fabric Identification (VFID).

Synopis **virtual-fabric 1**

Operands None

Defaults None

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
```

See Also None

virtual-ip

Configures a virtual IP address for the virtual router.

Synopsis **virtual-ip** *A.B.C.D*

no virtual-ip *A.B.C.D*

Operands *A.B.C.D* Virtual IP address of the virtual router.

Default None.

Command Modes Virtual-router-group configuration mode.

Description Configures a virtual IP address for the virtual router. This virtual IP address is the IP address that an end-hosts sets as its default gateway. The virtual IP address must belong to the same subnet as the underlying interface. A maximum of 16 virtual IP addresses can be configured for VRRP; only one virtual IP address can be configured for VRRP-E. The session gets enabled soon as the first virtual-ip is configured.

Usage Guidelines You can perform this command for VRRP or VRRP-E. Use the **no** parameter with this command to delete the virtual IP address

Examples To assign a virtual IP address of 192.53.5.1 to the VRRP virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IP address of 192.53.5.1 to the VRRP-E virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int ve 20
switch(config-Ve-20)# vrrp-group-extended 1
switch(config-vrrp-extended-group-1)# virtual-ip 192.53.5.1
```

See Also **vrrp-group**

vlag ignore-split

Controls the ignore-split recovery functionality.

Synopsis **vlag ignore-split**

no vlag ignore-split

Operands None

Defaults This option is turned off by default.

Command Modes Port-channel configuration mode

Description When ignore-spilt-recovery is active, neither of the RBridges modify their actor SID when splitting or rejoining the vLAG. They both advertise VSID and keep both sides of the vLAG alive.

Usage Guidelines This command is only supported when the switch is operating in Brocade VCS Fabric mode. Use the **no vlag ignore-split** command to disable this functionality.

Examples

```
switch(config)# interface port-channel 27
switch(config-Port-channel-27)# vlag ignore-split
```

See Also None

vlan classifier activate group

Activates a VLAN classifier group.

Synopsis **vlan classifier activate group** *number* **vlan** *vlan_id*

no vlan classifier activate group *number*

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. Refer to "Usage Guidelines" below.

Defaults None

Command Modes Interface subconfiguration mode (fo, gi, port-channel, te).

Description Use this command to activate a VLAN classifier group for a specified VLAN.

Usage Guidelines On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Use the **no vlan classifier activate group** *number* command to remove the specified group.

Examples To activate VLAN classifier group 1 for VLAN 5 on a specific tengigabitethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/1
switch(conf-if-te-178/0/1)# vlan classifier activate group 1 vlan 5
```

To remove VLAN classifier group 10 from a specific port-channel interface:

```
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no vlan classifier activate group 10
```

See Also **interface, vlan classifier group**

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 None

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.

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). On the Brocade VDX 8770, the VLAN value can be 1 through 4086. VLAN IDs 4087 through 4094 are internally-reserved VLAN IDs. On all other Brocade VDX switches, the VLAN value can be 1 through 3962, as 3963 through 4094 are reserved.

Examples To add rule 1 to VLAN classifier group 1:

```
switch(config)# vlan classifier group 1 add rule 1
```

See Also None

vlan classifier rule

Creates a VLAN classifier rule.

Synopsis **vlan classifier rule** *rule_id* [[**mac** *mac_address*] | [**proto** {*hex_addr* **encap** {**ethv2** | **nosnapllc** | **snapllc**} | **arp encap** {**ethv2** | **nosnapllc** | **snapllc**} | **ip encap** {**ethv2** | **nosnapllc** | **snapllc**} | **ipv6 encap** {**ethv2** | **nosnapllc** | **snapllc**}]]

no vlan classifier rule

Operands

rule_id	Specifies the VLAN identification rule. The range of valid values is from 1 through 2556.
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.
proto	Specifies the protocol to use for the VLAN classifier rule.
hex_addr	An Ethernet hexadecimal value. The range of valid values is from 0x0000 through 0xffff
arp	Specifies to use the Address Resolution 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.
nosnapllc	Specifies to use the Ethernet version 2 non-SNA frames.
snapllc	Specifies to use the Ethernet version 2 with SNA frames.

Defaults None

Command Modes Global configuration mode

Description Use this command to dynamically classify Ethernet packets on an untagged interface into VLANs. Use the **no vlan classifier rule** *rule_id* command to delete the rule.

Usage Guidelines VLAN classifiers are created individually and are 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 ARP VLAN classifier rule:

```
switch(config)# vlan classifier rule 2 proto arp encap ethv2
```

See Also show vlan

vlan dot1q tag native

Enables the native VLAN.

Synopsis [no] **vlan dot1q tag native**

Operands None

Defaults The native VLAN is enabled.

Command Modes Global configuration mode

Description Use this command to enable or disable the native VLAN.

Usage Guidelines None

Examples To disable the native VLAN:

```
switch(config)# no vlan dot1q tag native
```

See Also switchport mode, switchport trunk allowed vlan

vlan-profile (AMPP)

Activates the VLAN profile mode for AMPP.

Synopsis **vlan-profile**

no vlan-profile

Operands None

Defaults None

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 Use the **no vlan-profile** command to delete the profile.

Examples

```
Switch(config)# port-profile sample-profile
Switch(conf-pp)# vlan-profile
```

See Also None

vnetwork vcenter MYVC discover

Explicitly starts the discovery process on the vCenter.

Synopsis **vnetwork vcenter MYVC discover**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description The discovery of virtual assets from the vCenter occurs during one of the following circumstances:

- When a switch boots up
- When a new vCenter is configured on the VDX switch and activated (activation turns on the timer processing, set to 180-second intervals.)
- When the discovery is explictly initiated with the CLI.

Use this command to explicitly start the discovery process on the specified vCenter.

Usage Guidelines None

Example None

See Also show port-profile, show vnetwork

vrrp-extended-group

Configures a virtual-router-extended group.

Synopsis **vrrp-extended-group** *group-ID*

no vrrp-extended-group *group-ID*

Operands *group-ID* A value from 1 to 128 that you assign to the virtual router group.

Default None.

Command Modes Ve interface subconfiguration mode.

Description Configures a virtual-router group and enters into the virtual router configuration mode.

Usage Guidelines You can perform this configuration on **ve** interface only. Use the **no vrrp-extended-group** *group-ID* command to remove a specific VRRP Extended group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

Examples The following example shows how to assign the ve interface with a vlan number of 20 to the virtual router extended group with the ID of 1. (First you must enable VRRP-E on the switch.)

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int ve 20
switch(config-Ve-20)# vrrp-extended-group 1
```

See Also **interface, interface Ve, virtual-ip**

vrrp-group

Configures a virtual-router group.

Synopsis **vrrp-group** *group-ID*

no vrrp-group *group-ID*

Operands

group-ID	A value from 1 to 128 that you assign to the virtual router group.

Default None.

Command Modes Interface subconfiguration mode (fo, gi, te, Ve).

Description Configures a virtual-router group and enters into the virtual router configuration mode.

Usage Guidelines Use the **no vrrp-group** *group-ID* command to remove a specific VRRP group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

Examples The following example shows how to assign the tengigabitethernet interface 101/1/6 to the virtual router group with the ID of 1. (First you must enable VRRP on the switch.)

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# interface tengigabitethernet 101/1/6
switch(config-if-te-101/1/6)# vrrp-group 1
```

See Also interface, interface Ve, virtual-ip

zoning defined-configuration alias

Creates or deletes a zone alias.

Synopsis **zoning defined-configuration alias** *aliasName*

member-entry *member* [; *member*] ...

no member-entry *member*

no zoning defined-configuration alias *zoneName*

Operands **alias** *aliasName* Specifies a zone alias.

member-entry *member*
Specifies the WWN of the device to be added to the zone alias.

Defaults None

Command Modes Global configuration mode

Zoning configuration sub-mode

Description Use this command to create a zone alias, to add one or more members to a zone alias, or to remove a member from a zone alias.

This command enters a subconfiguration mode, where you can specify the names of the zone alias members to be added to the defined configuration or removed from the defined configuration.

Use the **member-entry** *member* [*; member*] ... command in the subconfiguration mode to add one or more members to a zone alias. You specify the zone alias member by its WWN. When adding multiple members in a single command line, the members are added sequentially until all members are added or the first error is encountered.

Use the **no member-entry** *member* command to remove a member from a zone alias. You can remove only one member entry each time you enter the **no member-entry** command.

If you remove the last member from a zone alias and subsequently commit the configuration, the commit operation deletes the zone alias.

Use the **no zoning defined-configuration alias** *aliasName* command to delete a zone alias.

The **zoning defined-configuration alias** command changes the defined configuration. To save the configuration persistently, issue the **zoning enabled-configuration cfg-action cfg-save** command. For the change to become effective, enable the configuration with the **zoning enabled-configuration cfg-name** command.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge.

Examples To create a zone alias with one member:

```
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:00:01
```

To add two additional WWNs to the zone alias:

```
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry \
10:00:00:00:00:00:00:02;10:00:00:00:00:00:00:02;
```

To remove a WWN from a zone alias:

```
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# no member-entry 10:00:00:00:00:00:00:01
```

To delete a zone alias from the defined configuration:

```
switch(config)# no zoning defined-configuration alias alias1
```

See Also show running-config zoning defined-configuration

zoning defined-configuration cfg

Creates a new zone configuration or adds a zone to an existing configuration.

Synopsis

zoning defined-configuration cfg *cfgName*

member-zone *zoneName*[*; zoneName*]...

no member-zone *zoneName*

no zoning defined-configuration cfg *cfgName*

Operands

cfgName Specifies the name of the zone configuration.

member-zone *zoneName*
Specifies the name of a zone to be added to the configuration or removed from the configuration.

Defaults

None

Command Modes

Global configuration mode

Zoning configuration sub-mode

Description

Use the **zoning defined-configuration cfg** command to create a new zone configuration, to add new zones to an existing configuration, or to remove member zones from a configuration.

This command enters a subconfiguration mode, where you can specify the names of the member zones to be added to the configuration or removed from the configuration. Use the **member-zone** *zoneName*[*;zoneName*]...command in the subconfiguration mode to add one or more zones. When adding multiple zones in a single command line, the zones are added sequentially until all zones are added or the first error is encountered.

NOTE
Zone aliases are not valid zone configuration members. Adding an alias to an existing zone configuration will not be blocked. However, the attempt to enable a zone configuration that contains aliases will fail with an appropriate error message.

Use the **no member-zone** *zoneName* command in the subconfiguration mode to remove a member zone from the configuration. You can remove only one member zone each time you enter the **no member-zone** command.

If you enable a zone configuration, the members in that zone configuration must be populated with at least one zone member-entry (a WWN or an alias); otherwise the enable operation fails.

If you remove the last zone from the configuration and subsequently commit the configuration, the commit operation deletes the configuration.

Use the **no zoning defined-configuration cfg** *cfgName* command to delete a configuration.

The **zoning defined-configuration cfg** command changes the defined configuration. To save the configuration persistently, issue the **zoning enabled-configuration cfg-action cfg-save** command. For the change to become effective, enable the configuration with the **zoning enabled-configuration cfg-name** command.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but is always executed on the principal RBridge.

Examples To add two zones to a zone configuration:

```
switch(config)# zoning defined-configuration cfg cfg4
switch(config-cfg-cfg4)# member-zone zone2;zone3
```

To delete a zone from a zone configuration:

```
switch(config)# zoning defined-configuration cfg cfg4
switch(config-cfg-cfg4)# no member-zone zone2
```

To delete a zone configuration:

```
switch(config)# no zoning defined-configuration cfg cfg3
```

See Also zoning defined-configuration zone, zoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-none

zoning defined-configuration zone

Creates a new zone or adds a member to an existing zone.

Synopsis **zoning defined-configuration zone** *zoneName*

member-entry *member [; member]* ...

no member-entry *member*

no zoning defined-configuration zone *zoneName*

Operands **zone** *zoneName* Specifies the name of the zone to be configured.

member-entry *member*
Specifies the name of the zone member to be added to the zone. The zone member can be specified by a WWN or a by a zone alias.

Defaults None

Command Modes Global configuration mode

Zoning configuration sub-mode

Description Use this command to create a new zone, to add one or more members to a zone, or to delete a member from a zone.

This command enters a subconfiguration mode, where you can specify the names of the zone members to be added to the defined configuration or removed from the defined configuration.

Use the **member-entry** *member* [*; member*] ... command in the subconfiguration mode to add one or more members to a zone. You can specify the zone member by its WWN or by a zone alias. When adding multiple members in a single command line, the members are added sequentially until all members are added or the first error is encountered.

Use the **no member-entry** *member* command to remove a member from a zone. You can remove only one member entry each time you enter the **no member-entry** command.

If you enable a zone configuration, the members in that zone configuration must be populated with at least one member-entry; otherwise the enable operation fails. However, You can have a non-populated zone in a zone configuration if that zone configuration only exists in the defined-configuration and is not enabled.

If you remove the last member from a zone and subsequently commit the configuration, the commit operation deletes the zone.

Use the **no zoning defined-configuration zone** *zoneName* command to delete a zone.

The **zoning defined-configuration zone** command changes the defined configuration. To save the configuration persistently, issue the **zoning enabled-configuration cfg-action cfg-save** command. For the change to become effective, enable the configuration with the **zoning enabled-configuration cfg-name** command.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge.

You can define a zone member by its port WWN or node WWN. However, when creating an LSAN zone, you should use only port WWNs, because node WWNs cannot be exported to a remote fabric.

Examples

To add a WWN and an alias to a zone:

```
switch(config)# zoning defined-configuration zone zone3
switch(config-zone-zone3)# member-entry 11:22:33:44:55:66:77:84;alias1
```

To remove a WWN from a zone:

```
switch(config)# zoning defined-configuration zone zone3
switch(config-zone-zone3)# no member-entry 11:22:33:44:55:66:77:82
```

To remove an alias from a zone:

```
switch(config)# zoning defined-configuration zone zone3
switch(config-zone-zone3)# no member-entry alias1
```

To delete a zone from the defined configuration:

```
switch(config)# no zoning defined-configuration zone zone2
```

See Also

zoning defined-configuration cfg

zoning enabled-configuration cfg-action cfg-clear

Clears all zone configurations in the defined configuration.

Synopsis **zoning enabled-configuration cfg-action cfg-clear**

Operands None

Defaults None

Command Modes Global configuration mode.

Description Use this command to clear all zone information. All defined zone objects in the defined zone configuration are deleted. If you try to commit the empty defined zone configuration while a zone configuration is enabled, you are warned to first disable the enabled zone configuration or to provide a valid configuration with the same name.

After clearing the defined zone configuration with this command, use the **no zoning enabled-configuration cfg-name** command to clear the entire zoning configuration (both the defined zone configuration and the enabled configuration). If no current active zoning configuration exists, or you just want to clear the defined zone configuration, use the **zoning enabled-configuration cfg-action cfg-save** command to commit the transaction.

If the default zone access mode is No Access, the **zoning enabled-configuration cfg-action cfg-clear** command recreates the default zoning objects.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge.

Examples To clear the defined zoning database:

```
switch(config)# zoning enabled-configuration cfg-action cfg-clear
```

See Also zoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-save

zoning enabled-configuration cfg-action cfg-none

Synchronizes the zoned configuration with the DCMd configuration.

Synopsis **zoning enabled-configuration cfg-action cfg-none**

Operands None

Defaults This command has no default values.

Command Modes Global configuration mode.

Description Use this command to synchronize the configuration in the Zoned database with the configuration in DCMd database.

Usage Guidelines VCS mode with Fabric Distributed Services enabled is supported. VCS mode without Fabric Distributed Services enabled is not supported. Standalone mode is not supported.

This command can be entered on any RBridge in a VCS cluster, but is always executed on the principle RBridge.

Examples The following example synchronizes the version of the zoning database in zoned with the version in DCMd:

```
switch(config)# zoning enabled-configuration cfg-action cfg-none
```

See Also show running-config zoning enabled-configuration, zoning enabled-configuration cfg-action cfg-save

zoning enabled-configuration cfg-action cfg-save

Saves the defined configuration to persist across reboots.

Synopsis **zoning enabled-configuration cfg-action cfg-save**

Operands None

Defaults None

Command Modes Global configuration mode.

Description Use this command to save the current zone configuration persistently. This command writes the defined configuration and the name of the defined zone configuration to nonvolatile memory in all switches in the VCS Fabric.

The saved configuration is automatically reloaded at power on. If a configuration was in effect at the time it was saved, the same configuration is reinstalled with an automatic **zoning enabled-configuration cfg-name** command.

The **zoning enabled-configuration cfg-action cfg-save** command validates the effective configuration by performing the same tests as the **zoning enabled-configuration cfg-name** command on enabling the configuration. If the tests fail, an error message is displayed and the configuration is not saved.

This command commits the current transaction. Pending transactions are pushed to nonvolatile memory. Any empty zones or empty configurations are deleted.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric , but it is always executed on the principal RBridge.

Examples The following example saves the current zone configuration:

```
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

See Also zoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-transaction-abort

zoning enabled-configuration cfg-action cfg-transaction-abort

Aborts a current fabric-wide transaction.

Synopsis **zoning enabled-configuration cfg-action cfg-transaction-abort**

Operands None

Defaults None

Command Modes Global configuration mode.

Description Use this command to abort the current zoning transaction without committing it. All changes made since the transaction was started are removed and the zone configuration database is restored to the state before the transaction was started.

Usage Guidelines. This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but is always executed on the principal RBridge.

Examples To abort the current zone transaction:

```
switch(config)# zoning enabled-configuration cfg-action cfg-transaction-abort
```

See Also zoning enabled-configuration cfg-action cfg-save, zoning enabled-configuration cfg-name

zoning enabled-configuration cfg-name

Enables a zone configuration.

Synopsis **zoning enabled-configuration cfg-name** *cfgName*

no zoning enabled-configuration cfg-name

Operands *cfgName* Specifies the configuration to be enabled.

Defaults If no configuration is enabled, zoning is not implemented and default zoning applies.

Command Modes Global configuration mode.

Description Use this command to enable a specific configuration. Only one configuration can be enabled at a time.

If the operation fails, the previous state is preserved; that is, zoning remains disabled, or the previous effective configuration remains in effect. If the operation succeeds, the new configuration replaces the previous effective configuration.

Use the **no zoning enabled-configuration cfg-name** to disable the currently enabled configuration. The VCS Fabric returns to default zoning mode. In this mode, either all devices can access one another, or no device can access any other device, depending on if the default zoning mode is ALLACCESS or NOACCESS.

This command commits the current defined zone configuration to both volatile and nonvolatile memory.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge.

Examples To enable a zone configuration:

```
switch(config)# zoning enabled-configuration cfg-name myconfig
```

To disable the currently enabled configuration:

```
switch(config)# no zoning enabled-configuration cfg-name
```

See Also show running-config zoning defined-configuration, show running-config zoning enabled-configuration, zoning enabled-configuration cfg-action cfg-transaction-abort

zoning enabled-configuration default-zone-access

Sets the default zone access mode.

Synopsis **zoning enabled-configuration default-zone-access {allaccess | noaccess}**

Operands

allaccess	Sets the default zone access mode to All Access. Each device can access all other devices attached to the VCS Fabric.
noaccess	Sets the default zone access mode to No Access. No device can access any other device in the VCS Fabric.

Defaults The default zone access mode is set to All Access.

Command Modes Global configuration mode.

Description Use this command to display or set the default zone access mode. Setting the default zone mode initializes a zoning transaction (if one is not already in progress), and creates reserved zoning objects. For the change to become effective, you must commit the transaction with the **zoning enabled-configuration cfg-action cfg-save** command or the **zoning enabled-configuration cfg-name** command.

A default zone controls device access is in effect when zoning is not enabled. When a user-specified zoning configuration is not enabled, the default zone is in effect, allowing access to all devices or no devices. When a user-specified zone configuration is enabled, it overrides the default zone access mode.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any RBridge in a Brocade VCS Fabric, but is always executed on the principal RBridge.

Examples To set the default zone mode to All Access:

```
switch(config)# zoning enabled-configuration default-zone-access allaccess
```

See Also zoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-none